

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JOSHUA ADAM SCHULTE,

Defendant.

S2 17 Cr. 548 (PAC)

THE GOVERNMENT'S MOTIONS *IN LIMINE*

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York
One Saint Andrew's Plaza
New York, New York 10007

David W. Denton, Jr.
Sidhardha Kamaraju
Matthew Laroche
Assistant United States Attorneys
Of Counsel

TABLE OF CONTENTS

PRELIMINARY STATEMENT	2
BACKGROUND	4
I. October 2015 Through March 2016: Schulte’s Workplace Problems	5
II. Schulte Inappropriately Accessed and Altered DEVLAN.....	8
III. EDG Tries to Remove Schulte’s Administrative Privileges.....	9
IV. Schulte Prepares to Copy Classified Information from DEVLAN	11
V. April 20, 2016: Schulte Stole Classified Information from DEVLAN	13
VI. Schulte Transfers the Leaked Information	14
VII. Schulte’s Problems with EDG Management Continue and He Begins to Take Further Interest in WikiLeaks	15
VIII. Schulte Resigns From the CIA.....	17
IX. The Leaks	18
X. Schulte Lies to Law Enforcement	19
XI. Schulte Violates the Court’s Protective Order and Announces an “Information War” From Prison.....	21
ARGUMENT.....	21
I. Evidence of Schulte’s Anger at CIA Management and His Inappropriate Actions on DEVLAN is Admissible as Direct Evidence of the Charged Crimes and as Other Act Evidence	21
A. Applicable Law	22
B. Discussion	24
II. Evidence of Schulte’s Conduct at the MCC is Admissible as Both Direct Evidence and Rule 404(b) Evidence of the Charged Offenses	27
A. Relevant Facts	28
B. Applicable Law	35
C. Discussion	37
III. Expert Testimony about WikiLeaks Should Be Admitted at Trial	49
A. Applicable Law	49
B. Discussion	52
IV. Statements Schulte Made During the November 2017 Proffer Are Admissible	55
A. Applicable Law	56
B. Discussion	57

V. The Government Should Be Permitted to Introduce Video Evidence Demonstrating Certain Computer Commands.....	59
VI. Schulte Should Not Be Allowed To Elicit Testimony about The Purported “Overclassification” of Documents or Information	61
A. Applicable Law	62
B. Discussion	65
VII. If Schulte’s Expert Claims That the Government Withheld Information from Him, Then The Court Should Instruct the Jury That the Court Authorized the Government To Do So.....	70
VIII. The Government Provides Notice of Certain Areas of Cross-Examination and Extrinsic Evidence That May Be Implicated By Schulte’s Testimony	71
A. Applicable Law	71
B. Discussion	74
CONCLUSION.....	77

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

JOSHUA ADAM SCHULTE,

Defendant.

S2 17 Cr. 548 (PAC)

The Government respectfully submits this memorandum in support of motions *in limine* seeking the following rulings with respect to the upcoming trial of the defendant Joshua Adam Schulte:¹

1. Evidence of Schulte's disgruntlement at the Central Intelligence Agency ("CIA") and his inappropriate actions on CIA computer systems is admissible as both direct evidence and Rule 404(b) evidence of the charged offenses.
2. Evidence of Schulte's conduct in prison is admissible as both direct evidence and Rule 404(b) evidence of the charged offenses.
3. Expert testimony about the online organization WikiLeaks.org ("WikiLeaks") is admissible.
4. Schulte's statements during a proffer with the Government are admissible.
5. Video demonstrations of computer commands or actions taken by Schulte on CIA computer systems are admissible.
6. Schulte is precluded from eliciting testimony concerning whether documents are properly classified in this case, or whether the CIA conducted an appropriate classification review.

¹ The Government is submitting a single consolidated memorandum in support of its motions *in limine* described above. In addition, the Government is submitting a sealed unclassified motion regarding a jury issue.

7. In the event that Schulte elicits testimony that certain information was withheld from the defense, the Court will give an instruction indicating that the Court authorized the Government to withhold that material.

Finally, the Government also provides notice as to certain areas of cross-examination and extrinsic evidence that may be implicated by Schulte's decision to testify in this case or by arguments made by his counsel.

PRELIMINARY STATEMENT

Schulte is responsible for stealing, disclosing, and attempting to disclose a massive amount of classified information, and his actions have caused catastrophic harm to national security. Based on his own words, Schulte's motivation for doing so is clear—revenge against those who dared to cross him. As part of an "information war" that began at the CIA and continued through his detention at the Metropolitan Correctional Center ("MCC"), Schulte has engaged in an escalating series of retaliatory acts targeting his co-workers and supervisors at the CIA, agents with the Federal Bureau of Investigation ("FBI"), and, most recently, the United States writ large.

Schulte's conduct began during his time with the CIA. Furious with his management's response to Schulte's false claims concerning another employee, Schulte responded by breaking into CIA computer systems, stealing classified information (the "Classified Information") about the CIA's precious-guarded cyber-tool arsenal, and transmitting it to WikiLeaks, which subsequently disclosed it publicly between March and November 2017 (the "Leaks"). Later, after he was detained in this case, Schulte enlisted his family and other inmates to help him brazenly violate a protective order entered by the Court, and then, even after the Court admonished him, he doubled down and did it again, this time also illegally disclosing classified information. From prison, Schulte declared the aforementioned "information war" against the United States,

threatening to reveal all of the classified information he knew unless he was released and directing others to “send all your govt’s secrets [to] WikiLeaks.” In furtherance of this so-called “war,” Schulte smuggled contraband cellphones into the MCC, created encrypted email accounts and secret social media accounts, and drafted misleading “articles” for public dissemination that were not only filled with lies, including allegations that the FBI planted evidence against Schulte in this case, but also contained classified information.

Based on the foregoing and other conduct, Schulte is facing eleven charges in the upcoming trial, including (i) three counts of violating 18 U.S.C. § 793, in connection with his unlawful theft of classified information from the CIA and transmittal of that information to WikiLeaks (Counts One through Three, together the “WikiLeaks Charges”); (ii) another count of violating § 793, in connection with his unlawful disclosure and attempted disclosure of classified information from the MCC (Count Four, the “MCC Leak Charge”); (iii) four counts of violating 18 U.S.C. §§ 641 and 1030, in connection with Schulte’s unauthorized accessing of CIA computer systems and theft of classified information from therein (Counts Five through Eight, together the “Illegal Computer Access Charges”); (iv) two counts of violating 18 U.S.C. §§ 1001 and 1503, in connection with false statements Schulte made to the FBI during its investigation (Counts Nine and Ten, together the “Obstruction Charges”); and (v) one count of violating 18 U.S.C. § 401(3), in connection with his willful violation of the protective order (Count Eleven, the “Contempt Charge”).

BACKGROUND²

Schulte was a CIA employee for several years until he resigned on November 10, 2016. While at the CIA, Schulte worked within the Center for Cyber Intelligence (“CCI”), Engineering Development Group (“EDG”). Schulte’s responsibilities included developing classified cyber tools, including tools that were designed to, among other things, covertly exfiltrate (or retrieve) data from computers. In 2015 and 2016, Schulte also acted as a systems administrator of DEVLAN, the computer system on which EDG did much of its work. Schulte’s administrative privileges included acting as an administrator over certain computer programs run on DEVLAN and some of the servers on which DEVLAN was operated. These programs included a commercially-available suite of software known as Atlassian, which included programs named Confluence (EDG’s Wikipedia-like page in which users could post comments about the group’s work), Stash (the repository for, among other things, source code), Jira, Bamboo, and Crowd.³

Schulte’s administrative rights allowed him to manipulate DEVLAN in specific ways, including by controlling access to various parts of the system and transferring data. As an administrator, Schulte was also familiar with how and where DEVLAN was backed up.

² The Government respectfully submits that all of the testimony and other evidence described in this brief is admissible as direct evidence of the crimes charged. The Government hereby provides notice that it also intends to offer this evidence, in the alternative, pursuant to Rule 404(b), and it addresses much of that evidence independently in Part I below. The Government plans to continue to meet with potential witnesses between now and the trial, and will supplement this notice as necessary should the Government learn of additional information involving the defendant or other Rule 404(b) evidence.

³ The Classified Information disclosed by WikiLeaks came from Confluence and Stash.

Specifically, Schulte knew that DEVLAN was configured so that an automated daily backup (the “Backups”) of its contents was stored on another server.

The Government’s evidence at trial will establish that Schulte stole the Classified Information from DEVLAN, among other illegal conduct, after Schulte became infuriated with his co-workers and management at the CIA. In particular, the evidence is expected to show, among other things, the following:

I. October 2015 Through March 2016: Schulte’s Workplace Problems

In the summer and fall of 2015, Schulte began having significant problems at the CIA, which stemmed from certain management actions and an ongoing feud with another EDG employee (“Employee-1”). The problems escalated on October 30, 2015, when Employee-1 sent an email to his and Schulte’s branch supervisor (the “Branch Supervisor”) complaining about Schulte’s behavior in the workplace. Later that same day, Schulte sent the Branch Supervisor an email in which Schulte falsely claimed that Employee-1 was abusive towards Schulte and other employees, and that Employee-1 had made a death threat against Schulte (the “October 30 Email”). When the Branch Supervisor met with Schulte about this email, Schulte acknowledged that he had sent it to, in sum and substance, cover himself in case Employee-1 had filed a complaint against Schulte.

Schulte’s problems continued into early 2016. In February 2016, Schulte strongly disagreed with a management decision to enlist a contractor to build a tool that was similar to one that Schulte was attempting to develop, and forced his way into a meeting with the contractor over the objection of the Branch Supervisor. During the meeting, Schulte complained about the contractor potentially jeopardizing other tools and operations. After the meeting, Schulte sent

emails complaining about the situation, and he told others that he was going to cause problems because of it, including by filing a complaint with the CIA's Inspector General.

Around this time, Schulte's interpersonal problems with Employee-1 worsened. In late February 2016, and at Employee-1's request, the Branch Supervisor reassigned Schulte's work on a specific project to another developer. This angered Schulte, and, on March 1, 2016, he emailed CCI's security office ("Security") and complained that Employee-1 was abusive and had made death threats toward him. Schulte also forwarded to Security the October 30 Email (which he had previously acknowledged was sent as a cover in case Employee-1 complained about Schulte's own actions).

In the weeks that followed, Schulte grew angrier at what he perceived was his management's indifference to his claim that Employee-1 had threatened him. Schulte also began to complain about what, according to him, amounted to favoritism toward Employee-1, claiming, for example, that while the investigation was ongoing, Schulte was moved to an "intern desk," while Employee-1 had been moved to a "prestigious desk with a window." Eventually, on or about March 23, 2016, Schulte filed a motion for a protective order against Employee-1 in state court. The motion was temporarily granted pending a hearing.

As a result of the interim protective order, CCI management decided to reassign Employee-1 and Schulte to different branches within EDG. Schulte complained that he was being unfairly retaliated against because he had made a security complaint against Employee-1, and threatened to hire a lawyer if management did not respond to his complaints. On or about March 29, 2016, Schulte submitted a form to Security, notifying the group that he intended to meet with an attorney to pursue legal action and that the media might become involved. When asked why he anticipated

media attention, Schulte said, in substance and in part, that the media would be interested in an article titled “CIA Punishes Employee for Reporting Office Death Threats” and that the attorney had told him that “the media is an essential tool in many legal matters.”

Schulte continued to complain to CCI management after being transferred to a different branch within EDG. On or about March 29, 2016, Schulte sent an email to several high-level supervisors at CCI, in which he wrote, “I just want to confirm that this punishment of removal from my current branch is for reporting to security in which my life was threatened and/or for submitting a protective order against [Employee-1].” That same day, Schulte also wrote to the CIA’s Office of General Counsel to ask whether the agency required employees to wait 18 months after leaving the agency before they could reapply for a position as a contractor.

Meanwhile, the state court proceedings with respect to Schulte’s motion for a protective order progressed. On or about April 6, 2016, Schulte and Employee-1 appeared in state court in connection with Schulte’s motion. At the hearing, Schulte brought and showed to the judge emails that had been marked for internal CIA use only, for which Schulte had not sought authorization through the appropriate procedures to disclose. At the end of the hearing, the state court judge granted Schulte’s motion. Approximately two days after the hearing, on or about April 8, 2016, Security interviewed Schulte about the hearing. During that interview, Schulte told Security, in substance and in part, that he was being punished for reporting Employee-1’s conduct, that he would “go to the media” if forced into a corner, and that he would “do whatever I have to do to make the situation right” and to “shed light on this.” During that and other interviews with Security, some of which were video recorded, Schulte also persistently made false statements

about Employee-1, including accusing Employee-1 of making racist and derogatory comments about his co-workers and even a co-worker's wife.⁴

II. Schulte Inappropriately Accessed and Altered DEVLAN

On or about April 4, 2016, after Schulte had been moved to a different branch in EDG, Schulte's administrative privileges to two projects overseen by the previous branch, Project-1 and Project-2, were revoked. Approximately ten days later, on or about April 14, 2016, Schulte confronted another server administrator ("Server Administrator-1") about Schulte's loss of administrative privileges to Project-1. Server Administrator-1 informed Schulte that because Schulte had been moved to a different branch, Schulte no longer required administrative privileges to Project-1. Schulte disagreed, and claimed that even though he had moved to another branch, he was still assigned to all of the projects that he had previously been working on. Server Administrator-1 explained that he had a different understanding but that Schulte could speak with the Branch Supervisor, Schulte's former supervisor, about it. Schulte then spoke with the Branch Supervisor, but did not raise the issue of administrator privileges, about which he had complained to the Server Administrator.

After his conversation with the Branch Supervisor, Schulte falsely told Server Administrator-1 that the Branch Supervisor had approved the reinstatement of Schulte's

⁴ Numerous employees have said that Schulte regularly made racist and abrasive comments toward his co-workers, and Employee-1 believes that at least part of the reason that Schulte targeted him was because Employee-1 is a minority. Schulte also wrote a number of racist statements in his prison notebooks. The Government does not intend to elicit Schulte's racist statements in its case-in-chief, unless Schulte opens the door to the introduction of this evidence at trial. For example, to the extent the defendant intends to assert that he was a model employee or that he was truthful with the CIA during the agency's internal investigations, then the Government may seek to elicit evidence of Schulte's racism, including his statements concerning Employee-1 and others.

administrative privileges to Project-1. Server Administrator-1 responded that he would discuss the issue with the Branch Supervisor, to which Schulte replied, in sum and substance, that Server Administrator-1 should restore Schulte's privileges now because Schulte was eventually going to regain access to Project-1 anyway. Server Administrator-1 and the Branch Supervisor then discussed the issue, and Server Administrator-1 emailed Schulte to inform him that, in fact, Schulte's administrative privileges to Project-1 would not be restored. Schulte responded by again requesting that his supervisors authorize him to continue to serve as an administrator for Project-1.

Unbeknownst to anyone at EDG, however, on April 14, after discussing the issue with Server Administrator-1 and the Branch Supervisor but before sending his response to Server Administrator-1's email, Schulte himself restored his privileges to Project-1, using administrative privileges that Schulte still possessed at that point. Server Administrator-1 discovered that Schulte had restored his privileges later that evening, and reported the incident to his management, who in turn raised the issue with Security. Schulte's actions caused significant concern within CCI because they were in direct violation of CIA policy and called into question whether Schulte could be trusted with classified information.

III. EDG Tries to Remove Schulte's Administrative Privileges

In response to Schulte's actions, CCI management tasked Server Administrator-1 and two other system administrators ("Server Administrator-2" and "Server Administrator-3," together with Server Administrator-1, the "Server Administrators") with removing all of Schulte's administrative privileges on DEVLAN. On or about April 16, 2016, the Server Administrators began the process of purging the administrator passwords and access points used by administrators,

including Schulte, to access DEVLAN as an administrator. Prior to deleting and creating new passwords, however, the Server Administrators created a “snapshot” of the Confluence database (the “April 16 Snapshot”). The April 16 Snapshot was a copy of the Confluence database as it existed on April 16 so that if any of the changes made to the system caused problems going forward, the Server Administrators could revert the system to the April 16 Snapshot and start over without doing lasting damage to the system.

As part of their work, the Server Administrators changed the administrator passwords and removed some of the administrative secure shell (“SSH”) Keys, which were another method for administrators to access DEVLAN, and generated new ones. As a result of this change, Schulte could no longer access the database directly to make changes to these program databases from within.

The Server Administrators, however, were unaware that the SSH Keys that they had removed, however, were only the ones that were used to log into the Atlassian Suite programs (Confluence, Stash, Jira, Bamboo, and Crowd). The SSH Key that Schulte (the “Schulte ESXi Key”) used to log into the ESXi server—which was the server that ran some of the Atlassian programs, including Confluence—was stored in a different location than the Atlassian SSH Keys that the Server Administrators had purged, and thus, the Server Administrators mistakenly did not remove it. Because the Schulte ESXi Key had been left intact, Schulte could still log on to the ESXi Server as an administrator, which allowed him to, among other things, make changes to the Atlassian Suite programs that were hosted on the ESXi Server. In other words, before April 16, Schulte had been able to access all of the Atlassian Suite programs as an administrator directly and exercise administrative privileges for those programs specifically. After April 16, Schulte had

administrative access to the Atlassian Suite programs only through the ESXi Server (which the Server Administrators did not realize), and had only limited privileges with respect to those programs (because the Server Administrators had removed his program-specific administrative privileges on April 16).

In addition to the partial removal of Schulte's administrative privileges for the Atlassian suite databases, on April 18, 2016, a division supervisor within EDG (the "Division Supervisor") also confronted Schulte about his actions concerning Project-1. At approximately 11:00 a.m. that day, the Division Supervisor met with Schulte and gave him a memorandum titled "Self-Granting Previously Revoked Admin Privileges on an Agency Computer Network" (the "Privileges Memorandum"). The Privileges Memorandum, in substance and in part, described Schulte's unauthorized restoration of his administrative privileges to Project-1 and stated: "do not attempt to restore or provide yourself with administrative rights to any project and/or system for which they have been removed." Schulte signed the Privileges Memorandum, acknowledging that he understood its prohibitions.

IV. Schulte Prepares to Copy Classified Information from DEVLAN

Almost immediately after the meeting with the Division Supervisor, Schulte began to try to access various parts of DEVLAN as a system administrator, knowing that he was prohibited from doing so. Although his attempts to log into the Atlassian Suite of programs as an administrator were unsuccessful, Schulte successfully logged into the ESXi Server using the Schulte ESXi Key approximately 15 minutes after meeting with the Division Supervisor. At approximately 1:00 p.m. that same day, Schulte emailed the Division Supervisor, writing that he had "verified that all private keys with access have been destroyed/revoked" and that "[i]t seemed

like overnight all my permissions within the products were removed and all my permissions on the servers themselves revoked. And all without anyone informing me.” Those statements were demonstrably false because, at the time Schulte sent this email and unbeknownst to his supervisors, he was logged into the ESXi Server as an administrator.

Approximately an hour after sending the email to the Division Supervisor, Schulte began to conduct searches on the Internet related to file transfers on Linux, such as, “copying multiple files linux [the operating system for part of the Atlassian Suite] large files,” “linux copy file over network,” and “linux copy large files hash.” Schulte then visited related websites, including a website titled, in part, “how to copy a large number of files quickly between two servers.” At approximately 4:54 p.m., Schulte conducted Internet searches for a “driver,” which is a type of computer program that was necessary to allow a computer to connect to the Internet (thus potentially allowing the computer to transfer data online).

On April 18, 2016, the Division Supervisor also emailed the EDG staff (including Schulte) to inform the group that going forward there would only be two Server Administrators for the Atlassian Suite. Later that evening, Schulte again used the Schulte ESXi Key to inappropriately log into the ESXi server. Around the same time, Schulte used a program that allowed him to view and edit log files that had been generated by the ESXi server. The log files that Schulte reviewed included logs that document (i) information about every computer command (*i.e.*, instructions to the computer) that was entered into the system, such as the date and time of the command, and (ii) all login attempts to the server. By reviewing these files, Schulte was able to see precisely what activity the system would record.

V. April 20, 2016: Schulte Stole Classified Information from DEVLAN

On or about April 20, 2016, Server Administrator-1 sent an email to the EDG staff, including Schulte, informing the group that on or about April 25, 2016, the databases for the Confluence and Bamboo programs would be moved from the ESXi Server to a new server. This was a significant change to DEVLAN and for Schulte, who was familiar with the workings of the ESXi Server, and who, as described above, still secretly had administrative access to the ESXi Server. Once the change took effect, Schulte would no longer be able access the Confluence database through the ESXi Server using the mistakenly preserved Schulte ESXi Key.

At approximately 5:20 p.m., Schulte inserted a USB storage device (the “SanDisk Device”) into his computer workstation. Around 10 minutes later, Schulte logged into the ESXI Server again using the Schulte ESXi Key. Schulte then created a snapshot of the Confluence database (the “April 20 Snapshot”), which captured the state of the database at that time. Schulte next reverted the Confluence database to the April 16 Snapshot that the Server Administrators had created when they were attempting to purge the system of Schulte’s administrative privileges. In the reverted state, all of the Confluence administrative privileges that were in existence on April 16—including Schulte’s—were restored.

The Confluence database remained in the reverted state for more than an hour. For the duration of the reversion, Schulte’s administrative privileges to Confluence was fully restored, including his ability to access the Backups through a preset path available to administrators. At approximately 6:51 p.m., Schulte restored the system back to the April 20 Snapshot. By restoring the current system, Schulte erased all record of what he had done during the hour that the system was reverted to the April 16 Snapshot. Schulte then deleted the April 20 Snapshot itself, as well

as the logs on the ESXi Server that showed that he had created the April 20 Snapshot, and reverted the system to the April 16 Snapshot. The following day, on or about April 21, 2016, Schulte repurposed the SanDisk Device that had been plugged in while the system was reverted to the April 16 Snapshot, wiping it clean. The ultimate impact of Schulte's conduct on the April 20 was surreptitiously to restore his access to the Classified Information for more than an hour and then to destroy all evidence of Schulte's activities on the system while his access had been restored.⁵

VI. Schulte Transfers the Leaked Information

On or about April 22, 2016, Schulte learned that Employee-1 was appealing the state court's granting of Schulte's motion for a protective order and that Security had closed its investigation into Schulte's false claim that Employee-1 had threatened his life. The following day, Schulte used a computer program called "Eraser Portable" to securely delete a folder from his home computer that was named for one of the cyber tools that Schulte had helped develop at EDG ("Project-2").

On or about April 24, 2016, Schulte downloaded to his home computer a program called "Tails," which is an acronym for "The Amnesic Incognito Live System." Tails works in conjunction with an online browser called "The Onion Router" or "TOR," which is designed to encrypt users' Internet traffic and make it difficult to determine their location. The combination of TOR and Tails allows a user to make anonymous connections to the Internet, thereby allowing the user to visit websites or transfer data without leaving a digital footprint. In fact, WikiLeaks lists Tails on its website as one of its "partner organizations."

⁵ As the Government will show at trial, Schulte's attempts to cover his tracks failed, and he, despite his deletion efforts, left some evidence of his activities on the system.

On or about April 28, 2016, Schulte again used Eraser Portable—the secure deletion program—on his home computer. This time, Schulte securely deleted five folders on his home computer that were named “data2.bkp,” “data3.bkp,” “data4.bkp,” “data5.bkp,” and “data6.bkp.” That naming convention—“data.bkp”—is one that Schulte used for files that he had encrypted on his home computer, including child pornography. Two days later, on or about April 30, 2016, Schulte conducted online research about securely deleting data from hard drives and how to transfer large volumes of data. For example, late that evening, Schulte conducted Internet searches for “western digital wipe utility,” and “Samsung ssd wipe utility.” A “wipe utility” is a program designed to erase all data on a hard drive and Western Digital and Samsung are manufacturers of, among other things, computer hard drives, and “ssd” is an acronym for “solid state drive,” a type of hard drive. After conducting these searches, Schulte visited a website page titled “Kill Your Data Dead With These Tips and Tool.” The website discussed, among other things, “lots of ways to obliterate sensitive data from of [sic] your drive.” Early the following morning, at around 3:00 a.m. on or about May 1, 2016, Schulte visited a website titled “how can I verify that a 1tb file transferred correctly.”

On or about May 3, 2016, Schulte downloaded instructions to his home computer for sending files over the Internet using Tails (which he had downloaded a few days earlier) and TOR. Three days later, on or about May 6, 2016, Schulte reformatted his home computer, which had the effect of deleting most of the data on Schulte’s home computer prior to May 6.

VII. Schulte’s Problems with EDG Management Continue and He Begins to Take Further Interest in WikiLeaks

Throughout the summer of 2016, Schulte continued to cause problems with his management at the CIA. In late May 2016, after one of the Server Administrators mistakenly

restored Schulte's access to Project-2 at Schulte's request, Schulte in turn used his erroneously granted access to revoke privileges to the project for all other EDG employees, including the employee to whom Project-2 had been assigned, meaning that new code could not be developed for the tool by anyone but Schulte. When the Division Supervisor confronted Schulte on or about June 20, 2016, Schulte claimed that he should have access to Project-2, that his privileges were being removed secretly, and that he would "fight back." Two days later, Schulte met with senior members of CCI's management, including the chief and deputy chief of EDG (the "EDG Chief" and "Deputy EDG Chief," respectively). At that meeting, Schulte was given another written letter warning. Schulte said during the meeting that he disagreed with the letter's conclusions and refused to sign the letter.

On or about June 28, 2016, Schulte sent an email to three high-ranking CIA officials titled "Resignation over retaliatory management." In the email, Schulte complained that he was being retaliated against for reporting the purported death threat made by Employee-1. In or about July 2016, Schulte began to look for other employment, and was frequently out of the office. On August 22, 2016, Schulte appeared in state court on a hearing regarding the protective order against Employee-1. Employee-1 also attended the hearing, along with three of Schulte and Employee-1's co-workers who were prepared to testify in Employee-1's defense. Schulte made a number of false exculpatory statements concerning Employee-1, and at the end of the hearing, the protective order was dismissed on jurisdictional grounds.

Around this time, Schulte also began regularly to search for information about WikiLeaks. In the approximately six years leading to August 2016, Schulte had conducted one Google search for WikiLeaks. Beginning on or about August 4, 2016 (approximately three months after he stole

the Classified Information), Schulte conducted numerous Google searches for WikiLeaks and related terms and visited hundreds of pages that appear to have resulted from those searches. For example, in addition to searching for information about WikiLeaks and Julian Assange, its primary leader, Schulte also conducted searches using the search terms “narcissist snowden,” “wikileaks code,” “wikileaks 2017,” “shadow brokers,” and “shadow broker’s auction bitcoin.” “Snowden” was presumably a reference to Edward Snowden, the former NSA contractor who disclosed information about a purported NSA surveillance program, and “Shadow Brokers” was a reference to a group of hackers who disclosed online computer code that they purportedly obtained from the NSA, beginning in or about August 2016. Indeed, in contrast to the period before August 4, 2016, between that date and March 2017 (when the first of the Leaks occurred), Schulte conducted searches for Wikileaks and related information on at least 30 separate days.

VIII. Schulte Resigns From the CIA

On or about October 12, 2016, Schulte sent an email to another CIA employee with the subject line “ROUGH DRAFT of Resignation Letter *EYES ONLY*.” The email contained the text of an apparent resignation letter (the “Draft Resignation Letter”) that spanned approximately three single-spaced pages. In the Draft Resignation Letter, Schulte (falsely) claimed that he was resigning because he had expressed concerns about the security of DEVLAN to the EDG Chief and other members of Schulte’s management chain “for two full years,” but that those concerns had gone unaddressed. Schulte further wrote, “This left [DEVLAN] open and easy for anyone to gain access and delete our entire EDG source code repository or even easily download and upload it in it [sic] entirety to the internet Luckily, nothing happened, but it still illustrates the lack-of-security and pure ineptitude of [the EDG Chief].” Schulte also asserted that once this “failure

of leadership was discovered,” the EDG Chief tried to “evade responsibility and blame the decentralized and insecure [sic] environment entirely on [Schulte.]”

Approximately one month later, on or about November 10, 2016, Schulte officially resigned from the CIA. That day, he sent an email to the CIA’s Office of the Inspector General (the “OIG Email”). In the OIG Email, Schulte reiterated many of the same complaints contained in the Draft Resignation Letter against the EDG Chief and others, including management’s purported treatment of him and its supposed failure to address the “security concerns” Schulte had allegedly raised in the past.

IX. The Leaks

On or about March 7, 2017, WikiLeaks disclosed on its website the first of the Leaks. The first Leak contained information from Confluence. At the time of the release, WikiLeaks also issued a press release, in which it claimed that the information had been given to WikiLeaks by a “source” who wished to raise “policy questions that [the source says] need to be debated in public, including whether the CIA’s hacking capabilities exceeded its mandated powers and the problem of public oversight of the agency,” and who wanted to “initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons.” In several subsequent releases, the last of which occurred on or about November 17, 2017, WikiLeaks posted information on several EDG tools that had been stored in Stash. The Leaks are the largest illegal disclosure of CIA information in the agency’s history and, as noted above, caused catastrophic damage to national security.

At the time of the initial Leak, Schulte was employed in New York City. On the day of the initial Leak and in the days that followed, Schulte contacted several of his former EDG

colleagues. In those communications, Schulte (i) indicated that he knew almost immediately that the information published by WikiLeaks was a “dump” from Confluence; (ii) asked about the status of the CIA’s investigation into the initial Leak; (iii) stated that he believed that he was a suspect in the investigation; and (iv) expressed dissatisfaction that some of his former colleagues did not appear to believe his denials of responsibility for the Leak. In the days that followed the release, Schulte also conducted several Google searches for information about WikiLeaks, including searches for “wikileaks public opinion.”

X. Schulte Lies to Law Enforcement

Following the initial Leak, Schulte was interviewed by the FBI five times in the presence of counsel. During those interviews, Schulte, among other things, (i) claimed that the initial Leak was not severe because it only contained information from Confluence, rather than source code for completed projects; (ii) indicated that he believed that the information could have been taken from the backup files (which it was); (iii) asserted that he had reported security deficiencies to his supervisors (which he had not), who, according to Schulte, were incompetent; (iv) claimed that he had never kept material from EDG on his home computer and that he had never worked on Project-2 outside of EDG’s offices (even though he had securely deleted a folder from his home computer that had the same name as Project-2); (v) claimed that he did not have a copy of the OIG Email, which contained classified information, even though a copy of the OIG Email was recovered from his apartment; and (vi) denied ever making CIA systems vulnerable to the theft of data (even though he had secretly logged in as an administrator and deleted logs of his activities).

On or about August 22, 2017, Schulte was arrested on child pornography charges and released on bail. On or about November 8, 2017, Schulte appeared at a status conference before

the Court. The following day, Schulte contacted security officials at the CIA and claimed that he had been approached by someone who may have been a foreign intelligence officer. Schulte claimed that while he was traveling to Court for the status conference, an unknown individual (“FNU LNU”) approached him at Grand Central Station and stated, in substance and in part, that (i) Schulte was a great computer engineer at the CIA; (ii) the U.S. Government had “betrayed and bankrupted” Schulte; (iii) Schulte knew many of the CIA’s assets in FNU LNU’s country; and (iv) FNU LNU would contact Schulte in the future.

The following week, on or about November 17, 2017, the FBI interviewed Schulte about the purported contact with FNU LNU pursuant to a proffer agreement (the “November 2017 Proffer”). During that interview, Schulte said, in substance and in part, that (i) Schulte had been traveling to Court on or about November 8 via the subway (the “Train”) from Grand Central Station; (ii) at some point during the trip, the passengers on the Train were required to disembark at a particular subway station; (iii) Schulte then boarded another train; (iv) during the trip, although Schulte could not remember when, FNU LNU approached Schulte from behind and said “Schulte”; (v) FNU LNU told Schulte that FNU LNU knew that Schulte had “built the cyber program,” that “the government had betrayed and bankrupted you,” that Schulte knew the “assets by name in my country,” and that “we will be in touch”; (vi) Schulte was only able to give a vague description of FNU LNU; (vii) Schulte thought that FNU LNU’s approach was “the FBI fucking with him”; (viii) Schulte did not tell his attorneys about this incident, even though it had occurred shortly before he saw them in court; and (ix) Schulte had contacted the CIA because he had had a dream about the FBI monitoring how long it took him to report the incident.

Schulte’s account of a purported encounter with FNU LNU is contradicted by records from the Metropolitan Transportation Authority (the “MTA”) and video evidence that shows, among other things, that (i) there is no record of any forced disembarkation of passengers on board the Train, or any other train operating on that line, during the time period of Schulte’s travel; and (ii) Schulte boarded and exited a train that made only two stops between Grand Central Station and the courthouse—first at Union Square (the stop immediately following the Grand Central Station stop on an express train) and then at Brooklyn Bridge/City Hall (the next stop on the express line and the stop nearest the courthouse).

XI. Schulte Violates the Court’s Protective Order and Announces an “Information War” From Prison

After being charged in this case, Schulte continued to violate the law by blatantly violating a Court entered protective order (the “Protective Order”) on two occasions, and continuing to disclose and attempt to disclose classified information to others from prison. Schulte’s actions after being charged in this case, which are described in additional detail in Point II below, are consistent with his conduct at the CIA—namely, that when Schulte feels challenged, he retaliates and seeks revenge through an escalating series of acts concluding with the disclosure of national defense information to harm the United States.

ARGUMENT

I. Evidence of Schulte’s Anger at CIA Management and His Inappropriate Actions on DEVLAN is Admissible as Direct Evidence of the Charged Crimes and as Other Act Evidence

As described above, as part of its proof at trial, the Government intends to introduce evidence of numerous events that occurred at the CIA involving Schulte, including Schulte’s (i) apparent anger that in or about February 2016, the CIA had enlisted a contractor to build a tool

that was similar to one worked on by the defendant; (ii) false claim in October 2015 and again in March 2016 that Employee-1 had, among other things, threatened to kill Schulte; (iii) apparent anger with how the CIA responded to his allegations concerning Employee-1, including his discontent with being moved to another CIA branch in late March 2016 and losing permissions to Project-1 and Project-2 because of that move; (iv) inappropriate reinstatement of his privileges to Project-1 in mid-April 2016; and (v) unlawful use of administrative privileges to revoke others' accesses to Project-2 in June 2016. These categories of evidence are admissible as direct evidence of the charged offenses, and as "other act" evidence bearing on Schulte's motive, knowledge, intent, and absence of mistake pursuant to Federal Rule of Evidence 404(b).

A. Applicable Law

The Second Circuit has repeatedly held that evidence of uncharged criminal activity is admissible when it constitutes intrinsic or direct proof of a charged crime. Such evidence may be admitted if it provides the jury with background for the events alleged in the Indictment, or if it arose out of the same transaction or series of transactions as the charged offenses. *See, e.g., United States v. Gonzalez*, 110 F.3d 936, 941 (2d Cir. 1997) (holding that background evidence may be admitted to show the circumstances surrounding the events alleged in the indictment or to furnish an explanation of the understanding or intent with which certain acts were performed). "[E]vidence of uncharged criminal conduct is not evidence of 'other crimes, wrongs, or acts' under Rule 404(b) if that conduct is inextricably intertwined with the evidence regarding the charged offense. In such circumstances, the uncharged crime evidence is necessary to complete the story of the crime on trial, and, thus, appropriately treated as part of the very act charged, or, at least,

proof of that act.” *United States v. Quinones*, 511 F.3d 289, 309 (2d Cir. 2007) (quotations and citations omitted); *see also United States v. Carboni*, 204 F.3d 39, 44 (2d Cir. 2000).

Under Rule 404(b), “[e]vidence of a crime, wrong, or other act is not admissible to prove a person’s character in order to show that on a particular occasion the person acted in accordance therewith,” but it “may be admissible for another purpose, such as proving motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident.” Fed. R. Evid. 404(b). This Court has long followed “an inclusionary approach to evaluating Rule 404(b) evidence, which allows evidence to be received at trial for any purpose other than to attempt to demonstrate the defendant’s criminal propensity.” *United States v. Edwards*, 342 F.3d 168, 176 (2d Cir. 2003) (internal quotation marks and citation omitted). The Court may admit other acts evidence if “(1) it is introduced for a proper purpose; (2) it is relevant to the charged offense; (3) its prejudicial effect does not substantially outweigh its probative value; and (4) it is admitted with a limiting instruction if requested.” *United States v. Rutkoske*, 506 F.3d 170, 177 (2d Cir. 2007).

Finally, Rule 403 authorizes the exclusion of relevant evidence only if its “probative value is substantially out-weighed by the danger of . . . unfair prejudice, confusing the issues, misleading the jury, undue delay, wasting time, or needlessly presenting cumulative evidence.” Fed. R. Evid. 403. Under the rule, evidence is unfairly prejudicial “only when it tends to have some adverse effect upon a defendant beyond tending to prove the fact or issue that justified its admission into evidence.” *United States v. Figueroa*, 618 F.2d 934, 943 (2d Cir. 1980); *see also United States v. Brand*, 467 F.3d 179, 195 n.1 (2d Cir. 2006) (same). The Second Circuit has long made clear that “other act” evidence that is neither “more sensational” nor “more disturbing” than the charged crimes will not be deemed unfairly prejudicial. *United States v. Roldan-Zapata*, 916 F.2d 795, 804

(2d Cir. 1990); *see also United States v. Mercado*, 573 F.3d 138, 141-42 (2d Cir. 2009) (holding that evidence of uncharged sale of firearms was not unfairly prejudicial as it was “not especially worse or shocking than” the charged drug conspiracy). A district court has “broad discretion” over the admission of evidence. *United States v. Nektalov*, 461 F.3d 309, 318 (2d Cir. 2006).

B. Discussion

The evidence described above is admissible at trial. To start, evidence of Schulte’s unauthorized actions on DEVLAN concerning Project-1 and Project-2 serves as part of the bases for Count Eight, one of the Illegal Computer Access Charges, which charges Schulte with causing the transmission of a harmful computer code to DEVLAN. The evidence will show that Schulte unlawfully altered DEVLAN to grant himself access and deny others access to Project-1 and Project-2, which is exactly what he is charged with in Count Eight. Accordingly, this evidence is plainly admissible at trial. *United States v. Kahale*, 789 F. Supp. 2d 359, 381 (E.D.N.Y. 2009) (“[D]irect evidence of the crimes charged in the indictment is considered relevant and admissible without reference to Federal Rule of Evidence 404(b).” (citation omitted)).

All of the evidence described above is admissible as direct evidence of the WikiLeaks Offenses, Illegal Computer Access, and Obstruction Charges because it is “inextricably intertwined” with the evidence regarding those offenses and “necessary to complete the story of the crime[s] on trial.” *Quinones*, 511 F.3d at 309. For example, evidence that Schulte was furious with management—because management used a contractor to complete a tool that Schulte could not; did not believe Schulte’s false claims concerning Employee-1; moved Schulte to another branch due to his conflict with Employee-1; or removed Schulte’s administrative privileges—is critical context necessary for the jury to understand why, when, and how Schulte stole the

Classified Information. This evidence also provides important background concerning Schulte's relationship with his supervisors that explains some of their actions (such as the removal of Schulte's privileges to certain programs and as an administrator); Schulte's response to those actions (such as Schulte secretly logging in as an administrator after he knew his administrative access was revoked); and Schulte's false statements to law enforcement following the initial Leak (such as that he had never worked on Project-2 outside of the CIA, despite evidence to the contrary on his home computer). Moreover, Schulte made incriminating statements in connection with these events, including his efforts to control Project-2, such as that he believed his administrative privileges had been secretly removed and that he would "fight back" because of it, which also constitute direct evidence of his guilt on the charged offenses. *See, e.g., United States v. Graziano*, 391 F. App'x 965, 967 (2d Cir. 2010) (admitting testimony in arson case that defendant had warned others that he was going to harm a business because defendant's business had been harmed as inextricably intertwined with charged offenses).

The foregoing categories of evidence are also independently admissible on several Rule 404(b) grounds. *First*, the fact that Schulte was furious with his management is highly probative of his motive to steal Classified Information in an effort to, in Schulte's words, "fight back" against perceived wrongs inflicted by CCI management. The evidence reflects Schulte's escalating series of retaliatory actions against others and reinforces his motive to commit the charged crimes: When Schulte became upset that Employee-1 was succeeding where Schulte was not, Schulte made false accusations against Employee-1; when those false accusations did not result in a management response that satisfied Schulte, Schulte made the same false claims in state court to obtain a temporary protective order; when obtaining the temporary protective order led to Schulte being

moved to another branch (against his wishes) and losing privileges to certain projects, Schulte inappropriately used his remaining administrative privileges to restore his lost privileges; and when Schulte lost all of his administrative privileges as a result, he stole the Classified Information and gave it to WikiLeaks. Courts regularly admit other acts evidence where, as here, it is relevant to showing a possible motive for the charged crimes. *See, e.g., United States v. Rahimi*, -- F. Appx. --, 2019 WL 5688217, at *3 (2d Cir. 2019) (evidence that defendant planted bombs in New Jersey was probative of “motive, intent, preparation, and planning in connection with his” detonation of bomb in Manhattan); *Graziano*, 391 F. App’x at 967 (affirming admission of prior threat by the defendant to prove the defendant’s motive and intent); *United States v. Bufalino*, 683 F.2d 639, 647 (2d Cir. 1982) (affirming admission of extortion threat made by defendant to prove his motive for seeking victim’s death); *see also United States v. Joy*, 192 F.3d 761, 768 (7th Cir. 1999) (defendant’s threat to potential accomplice that he had gun and that he intended accomplice to assist him in burglary was admissible to show defendant’s motive for subsequent possession of firearm that evening).

Second, and for similar reasons, the categories of evidence are also admissible under Rule 404(b) to demonstrate Schulte’s knowledge, intent, and absence of mistake. The Government expects that Schulte will argue at trial that his conduct on April 20, 2016 and other days has an innocent explanation and that, in any event, numerous other individuals had access to the classified information that was stolen. The fact that Schulte inappropriately re-obtained and used his administrative privileges to gain access to Project-1, and used then inappropriately re-obtained and used his administrative privileges to Project-2 to remove all others’ access to that project is relevant and admissible to show that Schulte also accessed DEVLAN on April 20 as an administrator for

unlawful purposes. *See, e.g., United States v. Morrison*, 153 F.3d 34, 57 (2d Cir. 1998) (affirming admission of uncharged bomb threat made by defendant to prove defendant’s knowledge, intent, and plan to threaten victim); *United States v. Jamison*, 299 F.3d 114, 121 n.3 (2d Cir. 2002) (affirming, in case involving Hobbs Act robbery, felon-in-possession, and use of a firearm in relation to a crime of violence charges, introduction of evidence of prior armed robbery, noting that defendant’s claim that firearm with which he shot victim belonged to co-defendant “put[] at issue whether Jamison ever had an intent to commit a robbery or to possess a weapon illegally”).

Finally, this evidence is not unfairly prejudicial. For the reasons set forth above, the evidence is highly probative of Schulte’s theft of the Classified Information and necessary to complete the story of the crimes charged. The evidence is also not “likely to arouse irrational passions,” *United States v. Smith*, 727 F.2d 214, 220 (2d Cir. 1984), because Schulte’s disputes with management and Employee-1, and his inappropriate actions with respect to Project-1 and Project-2, are no “more sensational,” *Roldan-Zapata*, 916 F.2d at 804, than stealing a massive amount of classified information and transmitting it to WikiLeaks.

II. Evidence of Schulte’s Conduct at the MCC is Admissible as Both Direct Evidence and Rule 404(b) Evidence of the Charged Offenses

As referenced above, while detained at the MCC, Schulte declared an “information war” against the United States. This so-called war had two goals: (i) to coerce the Government and the CIA to abandon this prosecution by publicly disclosing classified information until the Government relented; and (ii) to spread misinformation intended to portray Schulte as the victim of an attempted framing by the FBI and the CIA. Evidence of Schulte’s purported “information war” is admissible as both direct and Rule 404(b) evidence of the charged offenses, and

accordingly, the Government respectfully requests that the Court order that this evidence be admitted at trial.

A. Relevant Facts

1. Schulte Violates the Protective Order

On September 18, 2017, the Court entered a protective order (the “Protective Order”) governing the production of certain discovery in this case, based upon a determination that it was necessary to protect materials that, if disseminated to third parties, could jeopardize national security and the safety of others, as well as impede ongoing investigations. The Protective Order provides that Schulte and his defense team can use certain designated materials only to prepare his defense, and can disseminate protected materials only to specified individuals involved in the preparation of his defense. Schulte, through counsel, agreed to the terms of the Protective Order. The Government subsequently produced several search warrant affidavits in discovery that were subject to restrictions in the Protective Order (the “Protected Search Warrants”).

Despite the terms of the Protective Order, Schulte nevertheless caused to be disclosed at least one of the Protected Search Warrants to reporters with *The Washington Post* and *The New York Times*. On May 15, 2018, both *The Washington Post* and *The New York Times* published articles (the “*Post* Article” and the “*Times* Article”) concerning this case that discussed the content of at least one of the Protected Search Warrants. In a recorded telephone conversation from jail, Schulte also described the contents of one of the Protected Search Warrants to a reporter. When the reporter asked Schulte whether the Protected Search Warrants material was classified, Schulte responded that it was not, but stated that it was subject to the Protective Order. Recorded prison calls also showed that Schulte enlisted members of his family, including his cousin, to disseminate

one or more of the Protected Search Warrants, as well as what Schulte described as “articles” he had written. The Government subsequently recovered copies of at least some of these “articles” (the “Schulte Articles”) from Schulte’s family, including at least one “article” that included classified information (the “Classified Article”).

On May 21, 2018, at the Government’s request, the Court held a conference (the “May 21 Conference”). At the conference, the Court reiterated the terms of the Protective Order to Schulte and confirmed that Schulte understood the provisions of the Protective Order and the requirements it imposed on him. (*See* May 21 Conf. Tr. at 8). The Court also explicitly instructed Schulte, “If you want to vary the terms of the protective order, your relief is not to do it on your own, Mr. Schulte, but to have your lawyer come into court and explain why there should be a modification of the order.” (*See id.* at 7).

2. Schulte Wages His “Information War” from the MCC

Although initially released on bail, Schulte has been detained at the MCC since December 2017, when the Government learned that he had violated his bail conditions. While Schulte was detained at the MCC, he and other inmates arranged to have cellphones (the “Contraband Cellphones”) illegally smuggled into the prison for their use. Schulte coordinated his activities with other inmates, often using other inmates to obtain or store the Contraband Cellphones and using the Contraband Cellphones to pass messages covertly to other inmates. Schulte also used the Contraband Cellphones to create and access encrypted email accounts (the “Encrypted Email Accounts”) and social media accounts (the “Social Media Accounts”). In his own words, Schulte intended to use these accounts to engage in an “information war” against the United States by systematically disclosing classified information and materials designed to obstruct the

investigation and prosecution. For example, in journals found in Schulte’s MCC cell (the “Schulte Notebooks”), Schulte wrote the following:

- “If govt doesn’t pay me \$50 billion in restitution & prosecute the criminals who lied to the judge and presented this BS case then I will visit every country in the world and bear witness to the treachery . . . that is the USG [United States Government]. I will look to breakup diplomatic relationships, close embassies, and U.S. occupation around the world & finally reverse U.S. jingoism. If this one the way the U.S. govt treats one of their own, how do you think they treat allies?”
- “I NEED my discovery to be released to the public. I NEED my articles to be updated.”
- “The way is clear. I will set up [two blogs]. From here, I will stage my information war: . . . The [blog] will contain my 10 articles”

Schulte’s “information war” was no idle musing. Rather, Schulte used the Encrypted Email and Social Media Accounts to disseminate and attempt to disseminate classified information. For example, using one of the Encrypted Email Accounts, Schulte began to correspond with a reporter (the “Reporter”). In this correspondence, Schulte pretended to be a third person who was speaking on Schulte’s behalf and told the Reporter that he would give the Reporter “information” on several topics—including disclosures relating to high-ranking elected officials in the United States—if the Reporter published stories pursuant to a timeframe dictated by Schulte. For example, in one email Schulte wrote: “If you can consent to an embargo on disclosure of the information for a limited time we would give you an exclusive to the information spanning several topics.” In another email sent in September 2018, Schulte emailed the Reporter a copy of one of the Protected Search Warrants—even though Schulte previously had confirmed to the Court his understanding that the Protective Order prohibited this type of dissemination. Schulte also attached a document in which

he disputed facts contained in the Protected Search Warrant and in which he included classified information (the “Classified Search Warrant Document”).

Using the Contraband Cellphones, Schulte also began to post some of his writings on the Social Media Accounts. In these posts, Schulte asserted, among other things, that the Government had planted child pornography on his computer and that, through this prosecution, the “United States government has done the job of a foreign adversary to exploit its own intelligence officers.” Although the Government seized the Contraband Cellphones before Schulte was able to complete his plan, the Schulte Notebooks make clear that he intended to disseminate other classified material and misinformation. For example, the Schulte Notebooks include (i) a purported WikiLeaks article authored by a supposed FBI “whistleblower,” who claimed to have leaked Schulte’s discovery to WikiLeaks and to have knowledge that Schulte had been framed by the FBI and that the FBI had planted evidence of child pornography on Schulte’s personal computer (the “Fake FBI Document”); (ii) drafts of tweets allegedly written by one of Schulte’s former CIA colleagues, which disclosed classified information to bolster the alleged former colleague’s credibility and which claimed knowledge that Schulte had been framed, this time by the CIA (the “Fake CIA Tweets”); and (iii) a draft “article” in which Schulte criticized the FBI’s investigation and included classified information about Schulte’s training at the CIA (the “Malware Article”). Based on this conduct, the Government charged Schulte in the Indictment with Counts Four and Eleven.

3. The Government Collects Substantial Evidence of Schulte's Information War

The Government first learned of Schulte's misconduct in prison through another inmate ("CW-1"),⁶ who informed the Government that Schulte and at least one other inmate were using the Contraband Cellphones to communicate with individuals outside of the MCC. CW-1 described, in substance and in part, how Schulte used and stored multiple Contraband Cellphones, including how Schulte had encrypted one of the Contraband Cellphones with advanced encryption software. CW-1 also provided the Government with photographs and videos of Schulte, among others, using one or more of the Contraband Cellphones, as well as images of screenshots of one or more of the Contraband Cellphones that showed that the cellphones were being used to, among other things, transmit documents. The Government intends to call CW-1 and introduce some or all of these images at trial.⁷

After learning from CW-1 of this conduct, the Government executed several search warrants at the MCC.⁸ Through these searches, the Government found, among other things, one of the Contraband Cellphones (the "Samsung Phone") used by Schulte. Although the Samsung Phone was heavily encrypted, the Government was able ultimately to search it and found, among

⁶ At the time that the Government first met with CW-1, CW-1 had not entered into a cooperation agreement with the Government. Since that time, CW-1 has pleaded guilty to certain criminal offenses pursuant to a cooperation agreement.

⁷ In addition to CW-1, the Government also anticipates calling at least one other witness at trial who will testify about Schulte's conduct while at the MCC.

⁸ On October 18, 2019, the Court denied Schulte's motion to suppress the fruits of the MCC searches without a hearing. On October 31, 2019, the Court also denied Schulte's motion to suppress the search of his New York apartment, personal electronics, and personal electronic accounts.

other things: (i) evidence of Schulte's use of the Samsung Phone; (ii) evidence of the September 2018 email Schulte sent to the Reporter that attached the Protected Search Warrant and the Classified Search Warrant Document; (iii) evidence of additional communications with the Reporter, including encrypted communications in which Schulte claims to have been member of the group Anonymous, which is a group known for conducting cyber-attacks that has provided documents to WikiLeaks in the past; and (iv) evidence of encrypted messaging and secure deletion applications, including applications described in the Schulte Notebooks. The Government seeks to introduce this evidence from the Samsung Phone at trial.

In addition to the Samsung Phone, the Government also obtained the contents of and related information for the Encrypted Email and Social Media Accounts. These accounts contained, among other things:

- Evidence of Schulte's creation, maintenance, and use of the Encrypted Email and Social Media Accounts. For example, at least one of the Encrypted Email Accounts contained emails showing when some of the Social Media Accounts had been created and other communications from the providers of the Social Media Accounts.
- Evidence that Schulte tried to obscure his use of the Encrypted Email and Social Media Accounts. For example, login information for one or more of these accounts showed that they had been accessed from IP addresses in three different European countries all within a day's time.
- Evidence of Schulte's communications with the Reporter, including the September 2018 email Schulte sent to the Reporter that attached one of the Protected Search Warrants and the Classified Search Warrant Document, and the email in which Schulte—posing as a third party—claimed to have additional information that he would disclose to the Reporter if the Reporter would abide by Schulte's dictated publication schedule.
- Evidence of Schulte's posts on the Social Media Accounts. For example, one of the Social Media Accounts bears a photograph of Schulte and displays an article in

which Schulte claims that the FBI was seeking to frame him by planting child pornography on his personal computer (the “Word Press Post”).

The Government seeks to introduce the evidence related to the Encrypted Email and Social Media Accounts at trial.⁹

Finally, the Government also collected the Schulte Notebooks and the Malware Article, which were found by MCC officials in Schulte’s cell and provided to the FBI. The Schulte Notebooks—which are comprised of several notebooks and notepads—and the Malware Article contain, among other things:

- Evidence of Schulte’s desire to harm the United States through his “information war.” For example, Schulte explicitly described how he would use his “blog” and his “article” to wage his “information war” against the United States, and how he would seek to destroy the United States’ diplomatic relationships if he was not released from prison.
- Evidence of Schulte’s use and control of the Encrypted Email and Social Media Accounts. For example, on one page of the Schulte Notebooks, Schulte listed the Encrypted Email Accounts and their passwords. Similarly, on another page, Schulte wrote that he would need to “schedule tweets,” an apparent reference to scheduling Tweets to be posted to the Twitter account he created from the MCC.
- Evidence of the classified information Schulte intended to publicly disseminate. For example, the Schulte Notebooks contain the Fake Tweet, which Schulte appears to have drafted for dissemination over Twitter, and which includes classified

⁹ The Government has described the classified information underlying the MCC Leak Count—including the classified information in the Malware Article, the Fake Tweet, the Classified Search Warrant Document, and the Classified Article—to the Court and the defendant in classified submissions. As set forth in the Government’s CIPA Section 6(a) motion, which was filed on October 11, 2019, the Government has sought authorization from the Court to redact, summarize, or substitute portions of the classified information in the Malware Article, the Fake Tweet, the Classified Search Warrant Document, and the Classified Article for trial, and will submit its proposed substitutions to the Court and the defense under seal on November 26, 2019, the deadline for the Government’s CIPA Section 6(c) submission.

information about, among other things, at least one CIA cyber-tool. Similarly, the Malware Article—which similarly was plainly intended for public dissemination (particularly since it was addressed to the “tech industry”)—contains classified information about Schulte’s work at the CIA.

- Evidence of Schulte’s false exculpatory statements and intention to publicly disseminate these false statements as part of a disinformation campaign. For example, in both the Fake FBI Document and the Fake Tweet, Schulte claims (falsely) that the FBI and the CIA each tried to frame Schulte for the Leaks. Similarly, in another draft tweet, Schulte claims that another CIA employee—not Schulte—was responsible for the Leaks. The Schulte Notebooks also include evidence showing Schulte’s intent to leak his discovery and provide it to WikiLeaks as part of his misinformation campaign.
- Evidence of Schulte’s destruction of evidence. For example, Schulte wrote list of to-do items in the Schulte Notebooks, including to “delete suspicious emails.”
- Evidence of Schulte’s knowledge of non-public CIA information possessed by WikiLeaks. At multiple places in the Schulte Notebooks, Schulte claims that WikiLeaks has source code for at least one CIA cyber-tool that, although part of the data that the Government alleges Schulte stole and transmitted to WikiLeaks, was not publicly disclosed by WikiLeaks.

The Government seeks to introduce the non-privileged portions of the Schulte Notebooks at trial.¹⁰

B. Applicable Law

As noted above, Rule 404(b) allows the admission of uncharged crimes, wrongs, or other acts for purposes other than for proving propensity, “such as proving motive, opportunity, intent, preparation, plan, knowledge, identity, absence of mistake, or lack of accident.” Fed. R. Evid. 404(b). In the context of Rule 404(b), “identity” is “used as a shorthand for referring to proof of

¹⁰ A Government wall review team has redacted privileged information from the Schulte Notebooks and provided the redacted versions to the prosecution team. The prosecution team intends to introduce copies of these redacted versions, which may include Section 6 substitutions of classified information, as described above.

the doing of the criminal act by this defendant.” *United States v. Danzey*, 594 F.2d 905, 913 (2d Cir. 1979). Where identity is in issue, courts have routinely admitted evidence of other crimes evidence to establish the defendant as the perpetrator of the crime charged based on a common plan or scheme. *See, e.g., United States v. Sappe*, 898 F.2d 878, 877-80 (2d Cir. 1990) (evidence of previous bank robberies admissible to prove defendant was participant in charged conspiracy). The “similarity sufficient to admit evidence of past acts to establish a recurring *modus operandi* need not be complete; it is enough that the characteristics relied upon are sufficiently idiosyncratic to permit a fair inference of a pattern’s existence.” *United States v. Sliker*, 751 F.2d 477, 486-87 (2d Cir. 1984).

Moreover, “[e]vidence of a party’s consciousness of guilt may be relevant if reasonable inferences can be drawn from it and if the evidence is probative of guilt.” *United States v. Perez*, 387 F.3d 201, 209 (2d Cir. 2004). Consciousness of guilt evidence is admissible “if the court determines (1) the evidence is offered for a purpose other than to prove the defendant’s bad character or criminal propensity, (2) decides that the evidence is relevant and satisfies Rule 403, and (3) provides an appropriate instruction to the jury as to the limited purposes for which the evidence is introduced, if a limiting instruction is requested.” *Id.* (citing *United States v. Mickens*, 926 F.2d 1323, 1328-29 (2d Cir. 1991)). While false exculpatory statements alone are not sufficient to convict a defendant, “it is axiomatic that exculpatory statements, when shown to be false, are circumstantial evidence of guilty consciousness and have independent probative force.” *United States v. Parness*, 503 F.2d 430, 438 (2d Cir. 1974); *United States v. Gaskin*, 364 F.3d 438, 462 (2d Cir. 2004) (inference of criminal intent “was strengthened by [defendant’s] post-arrest false exculpatory statement denying ownership or knowledge of the [cash]”); *United States v.*

Glenn, 312 F.3d 58, 69 (2d Cir.2002) (false exculpatory statements may amount to “circumstantial evidence of consciousness of guilt and may strengthen inferences supplied by other pieces of evidence”). Similarly, “it is today universally conceded that the fact of an accused’s flight, escape from custody, resistance to arrest, concealment, assumption of a false name, and related conduct, are admissible as evidence of consciousness of guilt, and thus of guilt itself.” *United States v. Steele*, 390 F. App’x. 6, 12 n. 2 (2d Cir. 2010) (quoting *United States v. Myers*, 550 F.2d 1036, 1049 (5th Cir. 1977)) (internal quotation marks omitted). Moreover, evidence that a defendant sought to destroy or falsify evidence is admissible as evidence of consciousness of guilt. *See, e.g., United States v. Robinson*, 635 F.2d 981, 986 (2d Cir. 1980) (evidence that defendant directed another individual to sign false letter exonerating co-conspirators and to destroy passport that contained relevant evidence was admissible to show consciousness of guilt). Finally, evidence of witness intimidation also shows consciousness of guilt. *Mickens*, 926 F.2d at 1329.

C. Discussion

1. Evidence of Schulte’s “Information War” Is Direct Evidence of the Charged Conduct

The evidence of Schulte’s conduct in prison is direct evidence of the charged offenses, particularly the MCC Leak and the Contempt Charges. As described above, through its investigation, the Government discovered five categories of evidence of Schulte’s purported “information war,” including the following: (i) witness testimony, such as CW-1’s testimony about CW-1’s interactions with Schulte at the MCC; (ii) the Samsung Phone, including the chats recovered from that phone; (iii) the Encrypted Email and Social Media Accounts; (iv) the Schulte Notebooks; and (v) Schulte’s recorded calls from the MCC (the “MCC Calls”). These items contain direct evidence of the charged offenses, including among other things: (i) Schulte’s use of

the instrumentalities of his “information war” (the “Use Evidence”); (ii) the classified information that Schulte transmitted or attempted to transmit from the MCC (the “MCC Classified Information Evidence”); (iii) Schulte’s intent in his “information war,” *i.e.*, to harm the Government and the CIA so significantly as to force them to relent (the “Intent Evidence”); (iv) Schulte’s knowledge of non-public aspects of the CIA information WikiLeaks possesses (the “Nonpublic Information Evidence”); and (v) Schulte’s consciousness of guilt as to the WikiLeaks, MCC, and Contempt Charges (the “Guilty Conscience Evidence,” and together with the Use Evidence, the MCC Classified Information Evidence, the Intent Evidence, and the Nonpublic Information Evidence, the “MCC Evidence”).¹¹

First, to prove the MCC Leak Charge, the Government must show that Schulte transmitted or attempted to transmit national defense information. Similarly, to prove the Contempt Charge, the Government must show that Schulte willfully violated the Protective Order’s prohibition on disclosure of the Protected Search Warrant Materials outside of the defense team without court approval. The MCC Classified Information Evidence proves both of these elements. For example, the Samsung Phone and Encrypted Email Accounts contain evidence of the September 2018 email correspondence between Schulte and the Reporter (including the correspondence itself), in which Schulte transmitted some of the Protected Search Warrant Materials and the Classified Search Warrant Document to the Reporter. Similarly, the Prison Calls include at least one conversation between Schulte and a member of the media in which Schulte acknowledges—even before the

¹¹ The Schulte Notebooks also contain other evidence that the Government does not intend to elicit in its case-in-chief, but which could become relevant during a cross-examination of the defendant, *see infra* Part VIII.

May 21 Conference—that the Protected Search Warrant Materials were subject to the Protective Order. Furthermore, Schulte’s transmission of classified information to the Reporter coupled with a promise of more information to come, the creation and use of the Social Media Accounts to post some of his writings (like the Word Press Post), and his drafting of the Fake Tweets, Malware Article, the Schulte Articles, and “to-do lists” in which Schulte reminds himself to, among other things, “schedule” his tweets, establish—as required to make out an attempt theory—that Schulte took a “substantial step” toward the unauthorized transmission of national defense information. *See, e.g., United States v. Desposito*, 704 F.3d 221, 233 (2d Cir. 2013) (“Thus, a rational jury could find beyond a reasonable doubt that his persistent writing and mailing of letters constituted substantial steps toward obstructing his criminal trial.”).

Second, proving the MCC Leak Charge requires the Government to show that Schulte transmitted or attempted to transmit national defense information with reason to believe that the information could be used to injure the United States or for the benefit of a foreign nation. The Intent Information conclusively establishes this element. For example, Schulte’s declaration of his “information war” and stated plan to disrupt the United States’ diplomatic relationships in the Schulte Notebooks demonstrates that Schulte’s goal in disclosing national defense information from the MCC was to harm the United States, which of course shows that he had reason to believe that this disclosure could aid a foreign nation or harm the United States. Similarly, Schulte’s invitation to other U.S. government employees in the Schulte Notebooks to give their “govt’s secrets” to WikiLeaks if the employees felt mistreated and his veiled threats in the Social Media Accounts that the “United States government has done the job of a foreign adversary to exploit its own intelligence officers” is powerful evidence of Schulte’s desire to injure the United States

through his illegal disclosures, demonstrating that he had reason to believe that his disclosures could be used for that purpose.

Third, the Guilty Conscience Evidence demonstrates consciousness-of-guilt evidence with respect to the WikiLeaks, MCC Leak, and Contempt Charges. The Government expects to prove at trial that Schulte’s “information war” was an attempt to cow the Government and the CIA—the victim of both the WikiLeaks and MCC Leak Charges—into abandoning this prosecution. *Cf. Mickens*, 926 F.2d at 1329 (attempts to intimidate witnesses is evidence of consciousness of guilt). Moreover, the Guilty Conscience Evidence includes explicit proof of Schulte’s plans to destroy evidence, such as his reminder in the Schulte Notebooks to “delete suspicious emails,” which strongly undercuts any contention that Schulte’s conduct in prison was undertaken in good faith. *See Robinson*, 635 F.2d at 986 (evidence that defendant directed another individual to destroy passport that contained relevant evidence was admissible to show consciousness of guilt). Similarly, the Guilty Conscience Evidence is also replete with instances in which Schulte assumed a false identity, tried to obscure his use of the Encrypted Email and Social Media Accounts, and sought to shield his prison communications from scrutiny by law enforcement, such as Schulte’s use of the Contraband Cellphones, his communications with the Reporter as a third party, and his logging into the Encrypted Email Accounts from IP addresses that traced back to foreign countries, all of which rebuts an innocent explanation for Schulte’s conduct at the MCC. *See Steele*, 390 F. App’x. at 12 n.2 (assumption of a false name and related conduct proof of consciousness of guilt). Finally, Schulte’s attempts to create a disinformation campaign in which purported FBI and CIA employees attest to his innocence of the WikiLeaks Charges, shift blame to other CIA employees, and allege misconduct by the FBI and CIA—like the Fake FBI Document, the Fake CIA Tweets,

and some of the posts on the Social Media Accounts—are false exculpatory statements that show Schulte’s knowledge of his guilt of the WikiLeaks Charges. *See Parness*, 503 F.2d at 438 (false exculpatory statements admissible to show consciousness of guilt). Put simply, the surreptitious means by which Schulte conducted his “information war,” and the deceptive ends for which that “war” was intended, prove conclusively Schulte’s guilty purpose, and are thus relevant and direct evidence of the WikiLeaks, MCC Leak, and Contempt Charges.

Fourth, the Nonpublic Information Evidence also contains other direct evidence of the WikiLeaks Charges. The central issue at trial with respect to the WikiLeaks Charges is whether Schulte—as opposed to another party—stole and transmitted the Classified Information to WikiLeaks. The Government has alleged that Schulte stole and transmitted, among other things, a back-up file in which source code for multiple CIA cyber tools was compiled, only some of which WikiLeaks has disclosed. The Nonpublic Information Evidence consists of Schulte’s statements in the Schulte Notebooks that WikiLeaks is in possession of source code for a specific tool (which is one of the tools that played a role in the dispute between Schulte and Employee-1) that is contained in the back-up file that was stolen, even though WikiLeaks has not publicly disclosed that it possesses any source code for that tool. The fact that Schulte knows details about the theft that have not been publicly disclosed shows that he came by that knowledge in a unique way—namely, by committing the theft and leak.

Fifth, to hold Schulte accountable for any of the MCC Evidence, which constitutes direct evidence of the charged crimes, the Government must show that Schulte used the Contraband Cellphones, Encrypted Email and Social Media Accounts, and the Schulte Notebooks. The Use Evidence does just that. For example, CW-1’s testimony and related evidence establish that

Schulte was using smuggled cellphones in the MCC. The Samsung Phone, in turn, contains evidence of communications that pertain to Schulte's case or that are personal to Schulte, which shows that Schulte used the Samsung Phone (a cellphone that had been smuggled into the MCC). The Encrypted Email and Social Media Accounts, in turn, contain communications that are reflected in the Samsung Phone that pertain to Schulte's case or, in the case of Social Media Accounts, bear Schulte's photograph. Finally, the Schulte Notebooks—which were recovered from Schulte's cell—include, among other things, personal information about Schulte (which shows that the notebooks are his) and information about the Encrypted Email and Social Media Accounts (which shows that Schulte was using these accounts).¹²

2. Evidence of the “Information War” Is Also Admissible as Rule 404 (b) Evidence

The MCC Evidence is also admissible as Rule 404(b) evidence with respect to the WikiLeaks, MCC Leak, and Contempt Charges.

First, with respect to the WikiLeaks Charges, Schulte's contention that he is not the person who stole and transmitted the Classified Information to WikiLeaks creates a another basis for admitting the MCC Evidence—as proof of identity and *modus operandi* pursuant to Federal Rule of Evidence 404(b). *See United States v. Gubelman*, 571 F.2d 1252 (2d Cir. 1978) (“similar acts evidence” was relevant when defendant raised issue of identity); *see also Danzey*, 594 F.2d at 913

¹² Schulte also explicitly acknowledged his ownership and use of the Schulte Notebooks and the Encrypted Email Accounts in his civil filings against, among other entities, the Government, which are also party admissions that the Government can introduce against Schulte. To the extent Schulte attempts to dispute his use of these accounts, the Government may seek to introduce those portions of those civil filings.

(identity is “used as a shorthand for referring to proof of the doing of the criminal act by this defendant”). The circumstances of Schulte’s conduct in prison—especially his disclosure of classified information in response to a perceived wrong and through technologically savvy means—illustrate that Schulte was the one who, after growing disgruntled at the CIA, accomplished the technologically complicated task of stealing a massive quantity of classified information from a secure, isolated, CIA computer system, transmitting it to WikiLeaks, and deleting evidence of that transmission. Thus, in addition to as direct evidence of the WikiLeaks, MCC Leak, and Contempt Charges, the MCC Evidence is also independently admissible as Rule 404(b) evidence in support of the WikiLeaks Counts.

The MCC Evidence demonstrates a pattern of conduct that is highly probative of Schulte’s guilt of the WikiLeaks Charges. In both instances, Schulte grew infuriated with components of the U.S. government—the Schulte Notebooks show Schulte’s rage against the Government, the FBI, and the CIA for prosecuting him, while Schulte’s emails and interactions with other CIA employees in 2016 demonstrate his anger at the CIA for allegedly ignoring his complaints against Employee-1 and imposing related disciplinary measures. Similarly, in both cases, Schulte threatened to expose allegedly damaging information about the CIA to coerce the agency into acting as Schulte wished—from the MCC, Schulte declared his “information war” intended to destroy U.S. diplomatic relationships, while at the CIA, Schulte threatened to go to the media with a salacious story about the CIA purportedly ignoring Schulte’s (ultimately discredited) reporting of a death threat made against him. Furthermore, at both the CIA and the MCC, Schulte used technologically sophisticated means to conceal his actions, using encrypted accounts and

cellphones, and IP-masking techniques at the MCC and deleting logs and securely wiping removable media at the CIA.

The MCC Evidence shows that when aggrieved, Schulte responded with an “information war,” and when he wanted to operationalize that “information war,” his weapon of choice was the unauthorized disclosure of classified national defense information. The MCC Evidence also demonstrates that Schulte carried out his operation from the MCC in a technically sophisticated manner that was remarkably similar to his actions at the CIA. While the overlap between Schulte’s MCC and CIA conduct is not “complete,” the common aspects of Schulte’s conduct at both places is “sufficiently idiosyncratic to permit a fair inference of a pattern’s existence,” *Sliker*, 751 F.2d at 486-87, and thus, the MCC Evidence is admissible, pursuant to Rule 404(b), to show that Schulte was the one who stole and leaked the Classified Information, *see, e.g., United States v. Stevens*, No. S1 03 Cr. 669 (JFK), 2004 WL 2002978, at *2 (S.D.N.Y. Sept. 7, 2004) (“Evidence that in the past he robbed other banks, in New York City, committing the robberies within weeks of each other, threatening the use of a bomb and demanding money, tends to suggest that the defendant was the person who committed the robberies charged in the Indictment. In other words, this evidence goes to the issue of identity.”); *United States v. Hinton*, 31 F.3d 817, 822 (9th Cir. 1994) (admitting evidence of four previous assaults of victim under Rule 404(b) because “the charged and prior conduct were part of a pattern of abuse involving the same victim and . . . similar *modus operandi*”); *Sappe*, 898 F.2d at 877-80 (evidence that previous robberies involved threatening bank employees with toy gun and defendant was found with toy gun admissible to prove defendant’s participation in charged robbery conspiracy).

Second, with respect to the MCC Leaks and Contempt Charges, the MCC Evidence is also admissible as evidence of Schulte’s motive, intent, preparation, and planning. For example, the parts of the MCC Evidence in which Schulte discusses his anger with the U.S. government, his intention to declare an “information war” and to destroy the United States’ diplomatic relationships clearly show his motive for his conduct. *See, e.g., Morrison*, 153 F.3d at 57 (affirming admission of uncharged bomb threat made by defendant to prove defendant’s knowledge, intent, and plan to threaten victim). Similarly, Schulte’s carefully crafted plan to disclose classified information—drafting documents for dissemination in the Schulte Notebooks, creating the Encrypted Email and Social Media Accounts to broadcast that information, and arranging to use the Contraband Cellphones to use these electronic accounts secretly—is evidence of his “preparation” and “planning” for his “information war.” *See Rahimi*, 2019 WL 5688217, at *3 (evidence that defendant planted bombs in New Jersey was probative of “motive, intent, preparation, and planning in connection with his” detonation of bomb in Manhattan).

3. Rule 403 Does Not Bar Admission of the MCC Evidence

Finally, Federal Rule of Evidence 403 is no bar to admitting the MCC Evidence because there is nothing “unfairly prejudicial” about this evidence. To be sure, as set forth above, the MCC Evidence demonstrates facts that directly establish the defendant’s guilt, including his actual and attempted transmission of national defense information, his intent in doing so, and his consciousness of guilt. But the fact that evidence is “highly probative of guilt,” and thus plainly “prejudicial to the interests of that defendant,” does not support exclusion of evidence under Rule 403. *United States v. Gelzer*, 50 F.3d 1133, 1139 (2d Cir. 1995). Rather, for evidence to be “unfairly prejudicial,” it must “tend[] to have some adverse effect upon a defendant beyond tending

to prove the fact or issue that justified its admission into evidence.” *Figueroa*, 618 F.2d at 943. The MCC Evidence is not more sensational than evidence of Schulte’s theft of the Classified Information from the CIA and transmittal of that information to WikiLeaks. *See Roldan-Zapata*, 916 F.2d at 804 (2d Cir. 1990) (“other act” evidence is not unfairly prejudicial were it is neither “more sensational” or “more disturbing” than the charged offenses); *see also Mercado*, 573 F.3d at 141-42 (holding that evidence of uncharged sale of firearms was not unfairly prejudicial as it was “not especially worse or shocking than” the charged drug conspiracy).

Nor does the fact of the defendant’s incarceration render the MCC Evidence “unfairly prejudicial” because evidence of Schulte’s detention at the MCC is necessary to explain the background of the MCC and Contempt Charges and to explain the defendant’s motive to acting the way he did. *See, e.g., United States v. Mauro*, 80 F.3d 73, 76 (2d Cir. 1996) (trial court did not abuse discretion in admitting evidence of defendant’s incarceration to show background and defendant’s motive). For example, without eliciting Schulte’s incarceration, CW-1’s testimony about his interactions with the defendant would make no sense. *See United States v. Faison*, 393 F. App’x 754, 759 (2d Cir. 2010) (approving testimony from defendant’s co-conspirator that the two had shared a cell in prison; “[d]istrict courts have ‘discretion to admit evidence of prior acts to inform the jury of the background of the conspiracy charged, in order to help explain how the illegal relationship between participants in the crime developed, or to explain the mutual trust that existed between coconspirators’”) (quoting *United States v. Rosa*, 11 F.3d 315, 334 (2d Cir. 2003)); *United States v. Johnson*, No. S5 10 Cr. 431 (CM), 2010 WL 6091601, at *3-4 (S.D.N.Y. Nov. 15, 2013) (introducing evidence of defendant’s incarceration to explain how he met cooperating witnesses). The same is true of aspects of the MCC Evidence—the jury cannot

consider, for example, the MCC Calls or the need to use the Contraband Cellphones without learning of the defendant's incarceration. *See, e.g., United States v. Johnson*, No. S5 16 Cr. 281 (PGG), 2019 WL 690338, at *15 (S.D.N.Y. Feb. 16, 2019) (evidence of incarceration properly admitted where "evidence of incarceration is reflected in communications between co-conspirators") (citing *United States v. Guang Ju Lin*, 505 F. App'x 10, 12 (2d Cir. 2012)). The fact of the defendant's incarceration is too intertwined with the charged conduct to attempt to excise it from the trial.¹³

¹³ The introduction of this evidence about the defendant's incarceration does not raise any of the due process concerns at issue in *Estelle v. Williams*, 425 U.S. 501 (1976) and *Deck v. Missouri*, 544 U.S. 622, 629 (2005), as Schulte contended in his severance motion. Those cases deal with unconstitutional requirements that the defendant wear prison garb, *see Estelle*, 425 U.S. at 505, or be shackled, *see Deck*, 544 U.S. at 631-32, at trial, not the introduction of highly probative evidence of the crimes at trial. Construing the Due Process Clause to bar the introduction of relevant incarceration evidence would preclude the prosecution of a number of offenses that are predicated on such conduct, such as escape from a federal detention center, *see* 18 U.S.C. § 751(a), providing or possessing contraband in prison, *see* 18 U.S.C. § 1791, or inciting a riot at a federal prison, *see* 18 U.S.C. § 1792. Similarly, the Second Circuit's decision in *United States v. Deandrade*, 600 F.3d 115 (2d Cir. 2010) does not support excluding the MCC Evidence. In that case, the Second Circuit refused to vacate a conviction based on testimony from a cooperating witness about the defendant's incarceration because these references were "brief and fleeting," not intended by the prosecution, and "incidental to legitimate areas of inquiry." *See id.* at 119. But in *Deandrade*, the defendant was being tried for pre-incarceration narcotics trafficking—the defendant's prison conduct was not intertwined with the charged conduct. *See id.* at 116-17. In this case, however, Schulte's conduct at the MCC is inextricably intertwined with his incarceration—his criminal conduct occurred at the MCC and was tailored to defeat the MCC's security measures. Thus, *Deandrade* is inapposite. But even if, assuming for argument's sake, the defendant's incarceration could suggest an improper inference in the jury's mind, the solution would be to instruct the jury that it could only consider the defendant's incarceration for a limited purpose, and not criminal propensity, rather than preclusion of such obviously probative evidence. *See Mauro*, 80 F.3d at 76 (approving admission of evidence of defendant's incarceration where, among other things, trial court gave the jury a limiting instruction).

Certain parts of the MCC Evidence present a separate Rule 403 issue. Specifically, in some of the MCC Evidence—like the Fake FBI Document and the Word Press Post—Schulte claims that the FBI planted evidence of child pornography on his computer to frame him for the Leaks. As discussed above, Schulte’s invention of patently false stories to explain evidence of his criminal activity demonstrates consciousness of guilt. *See Parness*, 503 F.2d at 438 (false exculpatory statements admissible to show consciousness of guilt). At the same time, the Government acknowledges that the Court—with the Government’s consent—has severed the child pornography counts, in part to avoid prejudicing Schulte by introducing evidence of child pornography at the current trial. To address this issue, the Government submits that any references to child pornography in the prison evidence—or any other evidence at the January 2020 trial—be redacted and substituted. For example, the Government will redact the Fake FBI Document in such a way as to convey to the jury the fact that Schulte claimed that the FBI allegedly planted evidence of a different crime on Schulte’s computer, without specifying what that crime was. Similarly, the Government will introduce forensic evidence showing that the FBI found that certain files relevant to the WikiLeaks Charges were stored in the same highly-secured manner on Schulte’s personal computer as other evidence of a different crime, without specifying which crime. Finally, the Court could instruct the jurors that they are not to speculate as to what that different crime was, an instruction the jurors would be presumed to follow. *See United States v. Elfgeeh*, 515 F.3d 100, 127 (2d Cir. 2008) (jury is presumed to follow court’s instruction to disregard evidence). Taken together, these measures will prevent any prejudice to Schulte while preserving the Government’s ability to introduce this relevant evidence.

III. Expert Testimony about WikiLeaks Should Be Admitted at Trial

The Government has provided notice to the defendant that the Government intends to call at trial Paul Rosenzweig as an expert on WikiLeaks. Mr. Rosenzweig holds a number of positions, including as a Professorial Lecturer in Law at George Washington School of Law and as a Resident Senior Fellow for National Security and Cybersecurity at the think tank R Street. Previously, Mr. Rosenzweig served as the Deputy Assistant Secretary for Policy at the Department of Homeland Security, in addition to other public service. Mr. Rosenzweig will testify about (i) WikiLeaks's history, technical and organizational structure, goals, and objectives; (ii) in general terms, prior leaks through WikiLeaks, in order to explain WikiLeaks's typical practices with regard to receiving leaked classified information, its practices or lack thereof regarding the review and redaction of sensitive information contained in classified leaks, and certain well-publicized harms to the United States that have occurred as a result of disclosures by WikiLeaks; and (iii) certain public statements by WikiLeaks regarding the Classified Information at issue in this case. All of these are proper subjects of expert testimony, and the Court should authorize Mr. Rosenzweig to testify.

A. Applicable Law

Federal Rule of Evidence 702 allows an expert to offer testimony in the form of an opinion if the individual expert's "specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, as long as (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case." Fed. R. Evid. 702. An expert's testimony is admissible when (i) the expert has "sufficient qualifications to testify," *Humphrey v.*

Diamant Boart, Inc., 556 F. Supp. 2d 167, 174 (E.D.N.Y. 2008), and (ii) the proffered testimony has a “sufficiently reliable foundation.” *Davis v. Carroll*, 937 F. Supp. 2d 390, 412 (S.D.N.Y. 2013) (quoting *Amorgianos v. Nat’l R.R. Passenger Corp.*, 303 F.3d 256, 265 (2d. Cir. 2002)). “The Rules of Evidence provide a liberal standard for the admissibility of expert testimony,” *United States v. Dukagjini*, 326 F.3d 45, 52 (2d Cir. 2003), and the Second Circuit has held numerous times that expert testimony can be helpful to inform the jury about concepts involved in the trial that are “beyond the ken of the average juror.” *United States v. Lombardozzi*, No. S1 02 Cr. 273 (PKL), 2003 WL 1907965, at *4 (S.D.N.Y. Apr. 17, 2003); *see also United States v. Amuso*, 21 F.3d 1251, 1264 (2d. Cir. 1994).

This standard requires a “common sense inquiry into whether the untrained layman would be qualified to determine intelligently and to the best possible degree the particular issue without enlightenment from those having a specialized understanding of the subject involved in the dispute.” *United States v. Locascio*, 6 F.3d 924, 936 (2d. Cir. 1993). Undoubtedly, “expert witnesses are often uniquely qualified [in] guiding the trier of fact through complicated morass of obscure terms and concepts.” *United States v. Duncan*, 42 F.3d 97, 101 (2d Cir. 1994). However, as with all evidence, the Court retains the discretion to exclude expert testimony when its probative value is “substantially outweighed by the danger of unfair prejudice.” *Dukagjini*, 326 F.3d at 51-52.

Courts in this District and Circuit repeatedly have “approved the use of expert testimony to provide juries with background on criminal organizations,” *United States v. Farhane*, 634 F.3d 127, 159 (2d Cir. 2011), in particular “to help explain the operation, structure, membership, and terminology” of such organizations. *United States v. Mustafa*, 406 F. App’x 526, 528 (2d Cir.

2011). For example, in *United States v. Flores*, No. 15 Cr. 765 (PAC) (S.D.N.Y. 2016), this Court permitted expert testimony from a DEA agent at a cocaine-importation trial regarding drug trafficking patterns and methodologies. Expert testimony about the structure and workings of a group engaged in criminal activities is permissible either “as background for an offense [or] to assist in proving one or more elements of the offense.” *United States v. Mulder*, 273 F.3d 91, 101 (2d Cir. 2001). Courts have upheld the admissibility of expert testimony “(a) to help explain the operation, structure, membership, and terminology of organized crime families, (b) to explain the operations of drug dealers, and (c) to explain the structure of minority construction coalitions,” *United States v. Gentile*, 233 F. App’x 86, 88 (2d Cir. 2007) (collecting cases) (internal quotation marks and citations omitted), as well as to describe broad patterns of narcotics trafficking activity, *see, e.g., United States v. Hernandez*, 15 Cr. 379 (PKC), economic sanctions, *see, e.g., United States v. Atilla*, 15 Cr. 867 (RMB) (S.D.N.Y. 2017); *United States v. Vaghari*, 735 F. Supp. 2d 197, 203 (E.D. Pa. 2010) (admitting testimony of expert with “practical and academic experience in the area of Iran sanctions” “to testify about trans-shipment as a *modus operandi* in evading such sanctions”); terrorist organizations, *see, e.g., United States v. Ullah*, 18 Cr. 16 (RJS) (S.D.N.Y. 2018); *United States v. El Gammal*, 15 Cr. 588 (ER) (S.D.N.Y. 2017); *United States v. Rahimi*, 16 Cr. 760 (RMB) (S.D.N.Y. 2017); *United States v. Pugh*, 15 Cr. 116 (NGG) (E.D.N.Y. 2016), and “the role of charitable and non-governmental aid organizations in the Palestinian Territories, including their origins, their organization, governance, operations, and the needs to which they typically respond,” *Linde v. Arab Bank, PLC*, 922 F. Supp. 2d 316, 327 (E.D.N.Y. 2013).

B. Discussion

1. Mr. Rosenzweig Should Be Allowed to Testify

Mr. Rosenzweig's testimony will be directly relevant to the allegations in this case. Schulte is charged with transmitting the Classified Information to WikiLeaks "with intent or reason to believe that the information is to be used to the injury of the United States." Ind. ¶ 1. Accordingly, proof that it was foreseeable to Schulte that disclosure of classified information to WikiLeaks could cause "injury [to] the United States" is a critical element in this case. Indeed, the Senate Select Committee on Intelligence has explicitly stated "that WikiLeaks and its senior leadership resemble a non-state hostile intelligence service." S. Rep. 115-151 p. 10. In order to evaluate evidence related to this topic, the jury will need to understand what WikiLeaks is, how it operates, and the fact that WikiLeaks' previous disclosures have caused injury to the United States. The Government is entitled to argue that Schulte intended to harm the United States, by transmitting the stolen information to WikiLeaks, because he knew or had reason to know what WikiLeaks would do with the information. The fact that WikiLeaks' prior conduct has harmed the United States and has been widely publicized is powerful evidence that Schulte intended or had reason to believe that "injury [to] the United States" was the likely result of his actions—particularly given that the Government will introduce evidence that demonstrates Schulte's knowledge of earlier WikiLeaks disclosures, including his own statements.

The Government recognizes the need to avoid undue prejudice, and will therefore limit Mr. Rosenzweig's testimony to prior WikiLeaks leaks that have a direct relationship with particular aspects of the conduct relevant to this case, for example by linking specific harms caused by WikiLeaks in the past to Schulte's own statements of his intent to cause similar harms to the United

States or conduct. Those leaks include (i) the 2010 disclosure of documents provided to WikiLeaks illegally by Chelsea Manning; (ii) the 2010 disclosure of U.S. diplomatic cables; (iii) the 2012 disclosure of files stolen from the intelligence firm Stratfor; and (iv) the 2016 disclosure of emails stolen from a server operated by the Democratic National Committee. Notably, however, this testimony is far less likely to be inflammatory than expert testimony approved in other cases in this district, which has included, for example, “[t]estimony regarding attacks and plots perpetrated by al Qaeda, including the U.S.S. Cole and September 11, 2001 attacks.” *United States v. Mostafa*, No. 04 Cr. 365 (KFB), 2014 WL 1744717, at *4 (S.D.N.Y. Apr. 23, 2014).

Mr. Rosenzweig’s testimony will also provide context as to WikiLeaks’s role in the disclosure of the Classified Information. The operations of an online entity such as WikiLeaks are “beyond the ken of the average juror” and thus properly the subject of expert testimony, even though there has been media coverage of WikiLeaks and its activities. *See Amuso*, 21 F.3d at 1264 (“[d]espite the prevalence of organized crime stories in the news and popular media,” expert testimony concerning the “organization, structure, and terminology of organized crime families” was proper because “[a]side from the probability that the depiction of organized crime in movies and television is misleading, the fact remains that the operational methods of organized crime families are still beyond the knowledge of the average citizen”); *Farhane*, 634 F.3d at 159 (same with respect to expert testimony concerning the history and structure of al Qaeda). For example, expert testimony relating to WikiLeaks’ decentralized structure will help explain to the jury why the Classified Information Schulte stole was disseminated over a long period of time in multiple phases, notwithstanding the fact that Schulte stole the Classified Information from two backup files. Similarly, Mr. Rosenzweig will testify that WikiLeaks encourages online submissions

through particular forms of anonymous communication, including “Tails” and “TOR,” which is tradecraft that the Government expects to prove Schulte used in connection with the charged conduct. In this respect, Mr. Rosenzweig’s testimony is precisely the sort of testimony regarding “the operation, symbols, jargon, and internal structure of criminal organizations” that the Second Circuit has repeatedly approved. *United States v. Mejia*, 545 F.3d 179, 190 (2d Cir. 2008).

2. The Court Should Issue a Limiting Instruction about WikiLeaks’ Statements

As part of his testimony, Mr. Rosenzweig will also testify as to certain public statements by WikiLeaks in connection with the Leaks. These include statements on WikiLeaks’ official verified Twitter account and its website, wikileaks.org, that accompanied the disclosure of the Classified Information. For example, in or about February 2017, WikiLeaks began to post indications online that “Vault 7” was forthcoming. Similarly, as noted above, on March 7, 2017, the date of the first Leak, WikiLeaks issued a “press release,” in which it claimed that the information had been given to WikiLeaks by a “source” who wished to raise “policy questions that [the source says] need to be debated in public, including whether the CIA’s hacking capabilities exceeded its mandated powers and the problem of public oversight of the agency,” and who wanted to “initiate a public debate about the security, creation, use, proliferation and democratic control of cyberweapons.” Finally, with each of the Leaks, WikiLeaks also released an announcement through Twitter and its website, in which it supplied commentary about the Classified Information in the specific Leak.

These statements are out-of-court statements and—because there is no applicable hearsay exception—may not be offered for their truth. *See United States v. Harwood*, 998 F.2d 91, 98 (2d Cir. 1993). Because the jury may not consider these hearsay statements for their truth, the

Government intends to offer them only to prove the fact that WikiLeaks made them, when WikiLeaks made them, and the form in which they were published. The Government will not rely on the WikiLeaks statements for the truth of the content they contain. *United States v. Dupree*, 706 F.3d 131, 136 (2d Cir. 2013) (“[I]f the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted, and the statement is not hearsay.” (quoting Fed. R. Evid. 801(c), advisory committee’s note)); *see also Anderson v. United States*, 417 U.S. 211, 220 n.8 (1974) (“Of course, evidence is not hearsay when it is used only to prove that a prior statement was made and not to prove the truth of the statement.”).

Where, as here, a statement is not offered for its truth, the Court should instruct the jury as to the limited purpose for which the statement is admissible. *See* Fed. R. Evid. 105 (“If the court admits evidence that is admissible against a party or for a purpose—but not against another party or for another purpose—the court, on timely request, must restrict the evidence to its proper scope and instruct the jury accordingly.”). Accordingly, the Government respectfully requests that, after Mr. Rosenzweig describes the process by which he collected and reviewed WikiLeaks’ official statements, the Court instruct the jury that the content of the statements about which he will next testify may not be considered for the truth of the assertions contained therein, but only as evidence that the statements were made under the circumstances described.

IV. Statements Schulte Made During the November 2017 Proffer Are Admissible

As described above, on November 17, 2017, the FBI interviewed Schulte about his purported contact with FNU LNU, an unknown individual who Schulte suggested may have been a foreign intelligence officer (the “November 2017 Proffer”). During that proffer, Schulte demonstrably lied about the circumstances of the claimed interaction, including by making

incredible claims about a mandatory disembarkation of all passengers from the Train. Prior to the November 2017 Proffer, Schulte executed a proffer agreement with the U.S. Attorney's Office (the "Proffer Agreement"), which is attached as Exhibit A. The Proffer Agreement explicitly provides that the Government may use the defendant's statements "in a prosecution for false statements, obstruction of justice or perjury with respect to any acts committed or statements made during or after the meeting or testimony given after the meeting," as well as "for the purpose of cross-examination should [the defendant] testify" and "to rebut any evidence or arguments offered by or on behalf of" the defendant. Accordingly, pursuant to the terms of the Proffer Agreement, Schulte's statements during the November 2017 Interview are admissible (i) as direct evidence of the false statements in violation of 18 U.S.C. § 1001, as charged in Count Nine, and the obstruction of justice in violation of 18 U.S.C. § 1503, as charged in Count Ten, (b) should defense counsel make certain arguments as to Schulte's innocence, to rebut those claims at trial, and (ii) in cross-examination if Schulte elects to testify.

A. Applicable Law

"Like all contracts, proffer agreements must be interpreted to give effect to the intent of the parties." *United States v. Rosemond*, 841 F.3d 95, 107 (2d Cir. 2016) (internal quotation marks and citations omitted). Courts have repeatedly upheld the provisions of the Proffer Agreement at issue here, which permit the Government to cross-examine the defendant with his proffer statements and use those statements to rebut contrary arguments made by the defense. *See United States v. Mezzanatto*, 513 U.S. 196 (1995); *United States v. Lyle*, 919 F.3d 716, 732-33 (2d Cir. 2019). Moreover, it is well-settled in this Circuit that, once defense counsel makes a "factual assertion . . . that contradicts a statement made during the proffer session, the Government may

then offer the earlier proffer statement to rebut the assertion being made at trial.” *Rosemond*, 841 F.3d at 107.

“Case law confirms that proper rebuttal is not limited to direct contradiction.” *United States v. Barrow*, 400 F.3d 109, 120 (2d Cir. 2005). Rather, the concept is a broad one that encompasses “any evidence that the trial judge concludes fairly counters and casts doubt on the truthfulness of factual assertions advanced, whether directly or implicitly, by an adversary.” *Rosemond*, 841 F.3d at 108 (internal quotation marks and citations omitted); *Barrow*, 400 F.3d at 121 (“Rebuttal is hardly limited to evidence that directly contradicts what it opposes; rather, rebuttal encompasses any evidence that the trial judge concludes fairly counters and casts doubt on the truthfulness of factual assertions advanced, whether directly or implicitly, by an adversary.”). Indeed, to permit the defendant to present evidence or make arguments that are contrary to the admissions in his proffer session—without also permitting the jury to assess that evidence in light of that proffer—would thwart the truth-seeking purpose of a trial and mislead the jury. *See United States v. Gomez*, 210 F. Supp. 2d 465, 476 (S.D.N.Y. 2002) (“[E]nforcement of a proffer agreement does not preclude defense counsel from taking a position or presenting evidence inconsistent with a defendant’s proffer statements [b]ut if she does, . . . it is only fair that the Government then be permitted to present the defendant’s own words in rebuttal.”).

B. Discussion

There is no question that Schulte’s statements in the November 2017 Proffer are admissible. He has been charged with lying to federal officers during a proffer, and with obstructing the ongoing grand jury investigation of his conduct by doing so. Accordingly, as Schulte explicitly agreed when he signed the Proffer Agreement, his statements are admissible as

evidence of those charges. Moreover, if Schulte elects to testify—as he has repeatedly stated he intends to—any statements from the November 2017 Proffer are clearly proper grounds for cross-examination.

In addition, if the defense argues either that (i) someone other than Schulte committed the offenses described in the other charges in the Indictment, or that (iii) Schulte’s conduct is demonstrative of his innocence—particularly if the defense argues, as it has in its opposition to the Government’s motion pursuant to Section 6(a) of the Classified Information Procedures Act, that Schulte has shown “consciousness of innocence”—Schulte’s statements are also admissible to rebut such argument. It is well-established that “circumstantial evidence [of a defendant’s guilt] may include acts that exhibit a consciousness of guilt, such as false exculpatory statements.” *United States v. Gordon*, 987 F.2d 902, 907 (2d Cir. 1993). “While falsehoods told by a defendant in hope of evading prosecution are not themselves sufficient evidence on which to base a conviction, such falsehoods may strengthen an inference of guilt supplied by other evidence.” *United States v. Perez*, 387 F.3d 201, 209 (2d Cir. 2004); *see also United States v. George*, 779 F.3d 113, 122 (2d Cir. 2015) (“A factfinder could similarly infer consciousness of guilt from George’s efforts at obstruction.”).

The Second Circuit has explicitly held, for example, that “asserting, in an opening statement, that someone other than the defendant was the real perpetrator of the crime” is a “factual assertion[] that will trigger the” Government’s right to use a defendant’s proffer statements. *Rosemond*, 841 F.3d at 109. While Schulte is free to argue that the Government has not met its burden of proof, should he claim that someone else was actually responsible for the charged offenses, the Government is entitled to rebut that assertion with Schulte’s own false exculpatory

statements made during the proffer. Likewise, if the defendant argues that his actions after the charged conduct demonstrates a “consciousness of innocence,” fairness similarly dictates that the Government may prove Schulte’s consciousness of guilt—as reflected in his fantastical narrative of an approach by a purported foreign intelligence officer—to rebut that claim.

V. The Government Should Be Permitted to Introduce Video Evidence Demonstrating Certain Computer Commands

As described above, the Government’s evidence of the WikiLeaks Counts focuses on, among other things, actions that Schulte took on DEVLAN, including: (i) his unauthorized restoration of administrative privileges to Project-1 on April 14, 2016; (ii) his testing of his SSH key (*i.e.*, login credentials) to the ESXi server on April 18, 2016; (iii) his April 20, 2016 reversion of the Confluence database back to the April 16 Snapshot and then forward again to the April 20 Snapshot; and (4) his deletion of log files that showed his activities on the system during the April 20 reversion. To prove these events, the Government intends to introduce a host of forensic evidence—including log files and portions of computer memory—together with testimony from CIA employees familiar with the system and forensic and computer science experts.

During the testimony of one of the Government’s computer science experts, Patrick Leedom, the Government also intends to introduce several videos (the “Videos”) that Mr. Leedom created. The Videos depict Mr. Leedom entering the computer commands that are reflected in the forensic evidence that the Government intends to introduce, and will aid the jury in understanding that testimony. For example, in one of the Videos, Mr. Leedom shows what happens when he enters the same computer commands that Schulte entered on April 20, 2016, when Schulte deleted the log files. Similarly, in another of the Videos, Mr. Leedom illustrates the commands used to create the April 20 Snapshot and to move between two snapshots of a database, like the April 16

and April 20 Snapshots that Schulte used during his reversion of the Confluence database on April 20, 2016. Other Videos show the way in which an SSH key—like the one Schulte used to log into the ESXi server—is used to access a computer system. The Government will offer the Videos so that the jury can understand the highly technical aspects of Mr. Leedom’s testimony and the computer systems about which he will be testifying.

The Government respectfully submits that the Videos are admissible. In *Rahimi*, the Government offered a video depiction of the crime scene around a bomb-blast zone in Chelsea to help the jurors understand the dimensions of the scene and the locations where evidence was found. *See* 16 Cr. 760 (RMB) (S.D.N.Y. 2017). Courts have permitted experts to use video demonstrations of the use of machinery or tools that are not commercially available or familiar to the average juror. *See, e.g., Clevenger v. CNH Am., LLC*, 340 F. App’x 821, 825 (3d Cir. 2009) (“We find that the District Court did not abuse its direction in concluding that the probative value of [video in which expert operated a Case 85XT skid steer loader] was not substantially outweighed by the specter of either unfair prejudice to the Clevengers or misleading to the jury.”); *Veliz v. Crown Lift Trucks*, 714 F. Supp. 49, 51 (E.D.N.Y. 1989) (“[T]he Court admitted, again over plaintiff’s objection, certain videotapes, which depicted a lift truck carrying loads of varying weights to demonstrate the physical and mechanical principles involved in the braking of lift trucks.”); *Szeliga v. Gen. Motors Corp.*, 728 F.2d 566, 567 (1st Cir. 1984) (no error in admitting video evidence of accident during expert testimony). The same is true here—the Videos will enable the jury to understand ways in which DEVLAN, a type of computer system that is almost certainly not familiar to the average juror, responds to certain commands or actions that the Government will prove, through other evidence, Schulte took. Indeed, Schulte seems to concede

the utility of the Videos in his October 28, 2019 letter to the Court (the “October 28 Letter”), when he acknowledges that they could be used as demonstratives at trial.

The defendant’s objections to the introduction of the Videos, which were raised in a footnote in his October 28 Letter, are meritless. *First*, the defendant argues that the Videos should be excluded because they are based on material to which Schulte did not have access. That is wrong. To create the Videos, Mr. Leedom simply took information that was contained in the discovery produced to Schulte and inputted it into commercially available software that was used at the CIA and with which Schulte (and his expert) are familiar. Schulte could do the same thing. Aside from his conclusory statement, Schulte has not identified any piece of data or information that he purportedly is missing that stops him from doing so. *Second*, to the extent Schulte believes that the Videos do not accurately capture the way that DEVLAN operated, the Government is not offering the Videos as a reconstruction of events on the system, and “[d]issimilarities between experimental and actual conditions affect the weight of the evidence, not its admissibility.” *Szeliga v. Gen. Motors Corp.*, 728 F.2d 566, 567 (1st Cir. 1984) (approving introduction of video demonstration created by expert witness). Accordingly, the Government submits that the Videos should be admitted as evidence at trial.

VI. Schulte Should Not Be Allowed To Elicit Testimony about The Purported “Overclassification” of Documents or Information

In his CIPA Section 5 notice and some of the evidence from the MCC, Schulte indicated that he intends to argue at trial that the CIA deliberately over- or mis-classified documents to hinder his ability to defend himself both against the allegations that were made against him while at the CIA and against the charges in the Indictment. Such an argument is irrelevant, inflammatory,

and inappropriate, and Schulte should not be permitted to advance such an argument or elicit testimony or introduce evidence in support of this meritless claim.

A. Applicable Law

Article II, Section 2 of the Constitution provides that the “President shall be Commander-in-Chief of the Army and Navy of the United States.” The Supreme Court has recognized that the President’s “authority to classify and control access to information bearing on national security . . . flows primarily from this constitutional investment of power in the President and exists quite apart from any explicit congressional grant.” *Department of Navy v. Egan*, 484 U.S. 518, 527 (1988). The President has sought to protect sensitive information and to ensure its proper classification throughout the Executive Branch by issuing a series of Executive Orders establishing a classification system and delegating this responsibility to the heads of agencies. *Id.*

Accordingly, the classification of national security information is an executive function. That system has been governed by executive order, most recently Executive Order No. 13526, 75 Fed. Reg. 707 (Dec. 29, 2009). These orders “prescribe[] a uniform system for classifying, safeguarding, and declassifying national security information.” *United States v. Morison*, 844 F.2d 1057, 1074 (4th Cir. 1988). Executive Order 13526 sets forth the criteria for classifying information and describes the policies and procedures by which information essential to the nation’s security and foreign relations is protected from unauthorized use, dissemination, handling, and storage. Information can be classified if it:

- (1) is owned by, produced by or for, or under the control of the United States government;
- (2) falls within one or more of the categories set forth in Section 1.4 of the Executive Order (including intelligence sources and methods, cryptology, military plans, weapons systems and vulnerabilities or

capabilities of systems, installations, projects, or plans relating to the national security); and

(3) is classified by an original classification authority who determines that its unauthorized disclosure reasonably could be expected to result in damage to the national security.

The U.S. government instructs each individual whom it entrusts with access to classified information that the classification of information reflects a determination that, if disclosed without proper authorization, the information reasonably could be expected to cause damage to national security. Such individuals are further informed that classification levels are assigned based on the degree of damage such disclosure reasonably could be expected to cause: TOP SECRET for “exceptionally grave damage;” SECRET for “serious damage;” and CONFIDENTIAL for “damage.” *Id.* Classification markings also limit the population entitled to receive the classified information. *Morison*, 844 F.2d at 1074-75.

It is well-settled that neither courts nor defendants may challenge the Executive Branch’s classification decisions.¹⁴ *See, e.g., El-Masri v. United States*, 479 F.3d 296, 305 (4th Cir. 2007) (“[T]he courts, of course, are ill-equipped to become sufficiently steeped in foreign intelligence matters to serve effectively in the review of secrecy classifications” (quoting *United States v. Marchetti*, 466 F.2d 1309, 1318 (4th Cir. 1972))); *United States v. Smith*, 750 F.2d 1215, 1217 (4th Cir. 1984) (“[T]he government . . . may determine what information is classified. A defendant cannot challenge this classification. A court cannot question it.”); *United States v. Rosen*, 520 F.

¹⁴ These cases address defendants’ challenges to classification decisions in the discovery context. Of course, if the defendant is not entitled to challenge these decisions during the discovery process, there is no reason why he would legally be permitted to do so at trial.

Supp. 2d 786, 790 (E.D. Va. 2007) (“It is not open to the court to question or second-guess the classification status of any document. . . .”); *see also United States v. Moussaoui*, 65 F. App’x 881, 887 n.5 (4th Cir. 2003) (“Nevertheless, Intervenor maintain that we need not defer to the classification decisions of the Government. Implicit in this assertion is a request for us to review, and perhaps reject, classification decisions made by the executive branch. This we decline to do.”); *United States v. Kiriakou*, No. 12 Cr. 127 (LMB), Dkt. 62 (E.D. Va. Aug. 8, 2012) (“Regardless of whether the ‘government itself acknowledges that it over-classifies a great deal of information,’ as defendant argues, . . . the classification system is the purview of the executive branch; accordingly, the Court declines to second-guess the CIA’s classification decisions.” (citation omitted)).

In *Marchetti*, the Fourth Circuit explained the rationale supporting this deference to Executive Branch classification determinations:

The CIA is one of the executive agencies whose activities is closely related to the conduct of foreign affairs and to the national defense. Its operations, generally, are an executive function beyond the control of the judicial power. If in the conduct of its operations the need for secrecy requires a system of classification of documents and information, the process of classification is part of the executive function beyond the scope of judicial review.

466 F.2d at 1317.

Executive Branch agencies exercising original classification authority are uniquely positioned to assess the damage to the national security of information in light of the global context for such information. Courts and defendants do not have the same access to this global perspective. *See, e.g., United States v. Snepp*, 897 F.2d 138, 141 n.2 (4th Cir. 1990) (“Courts must avoid second-guessing the CIA’s decision to classify information because they have only a limited

knowledge of foreign intelligence matters.”); *see also El-Masri*, 479 F.3d at 307 (“The executive branch’s expertise in predicting the potential consequences of intelligence disclosures is particularly important given the sophisticated nature of modern intelligence analysis, in which the significance of one item of information may frequently depend upon knowledge of many other items of information, and what may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context.” (citation and quotations omitted)).

B. Discussion

Initially, neither the defendant, defense counsel, nor any individual witness is privy to all of the information that went into these classification decisions, and is thus not in a position to question them. *See Marchetti*, 466 F.2d at 1318. As the Fourth Circuit noted in *El-Masri*, the assessment as to whether there would national security consequences from the disclosure of any particular piece of information “may frequently depend upon knowledge of many other items of information, and what may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context.” 479 F.3d at 307 (citations and quotations omitted). Neither the defendant nor any of the witnesses at trial are privy to all of the information available to the U.S. intelligence community and used to make classification determinations. Thus, their particular view that a piece of information is not classified or was mis-classified is pure speculation.

With respect to Counts One through Four, the relevant question for the jury is not whether the information Schulte disclosed and attempted to disclose is properly classified but rather whether it is “national defense information” or “NDI.” *See* 18 U.S.C. 793(b) (information illegally

gathered must be NDI); (d) (information illegally transmitted must be NDI); & (e) (same). While “national defense” is not defined in § 793, courts have uniformly held that “national defense” is a “generic concept of broad connotations, referring to the military and naval establishments and the related activities of national preparedness.” *Gorin*, 312 U.S. at 28. In this vein, courts have held that the following types of information may qualify as NDI: (i) U.S. intelligence on the movements of Japanese citizens and officials during World War II, *Gorin*, 312 U.S. at 29; (ii) documents containing information about the anticipated movements of Navy ships, *United States v. Abu-Jihaad*, 630 F.3d 102, 135-36 (2d Cir. 2010); (iii) classified manuals for the installation and maintenance of guided missiles and bombs, *United States v. Drummond*, 354 F.2d 132, 151 (2d Cir. 1965); and (iv) information regarding how a U.S. intelligence agency “carried on its work and who did what [and] information with respect to the development of an important military weapon,” *United States v. Soblen*, 301 F.2d 236, 239 (2d Cir. 1962). Moreover, in order to qualify as national defense information, the information must be closely held by the Government (that is, not publicly available through lawful means). *United States v. Heine*, 151 F.2d 813, 817 (2d Cir. 1945) (holding that the dissemination of information that the Government had never kept secret cannot support an espionage conviction under § 793); *see also Abu-Jihaad*, 630 F.3d at 136.

To be sure, the fact that information is classified and handled accordingly can help to show that the information is closely held. *See, e.g., United States v. Dedeyan*, 584 F.2d 36, 40 (4th Cir. 1978) (finding no abuse of discretion in trial court’s admission of classification markings on document because the fact of classification tends “to show or make more probable that the document does, in fact relate to the national defense”) (internal citation and quotation omitted). However, “NDI . . . is not synonymous with ‘classified’; information that is classified by the

executive branch of government may or may not qualify as NDI.” *Rosen*, 599 F. Supp. 2d at 694. In other words, while the jury may take into account the fact that information is classified in determining whether the information was closely held, and thus potentially NDI, the fact of classification is not sufficient to establish that the information is national defense information. Evidence of classification can also provide evidence of *mens rea*—a trained member of the CIA, such as Schulte, would recognize classification markings and other indicia of classification as clear indications that the U.S. Government has decided to hold certain information closely for national security purposes. *United States v. Hitselberger*, 991 F. Supp. 2d 101, 106 (D.D.C. 2013); *United States v. Drake*, 818 F. Supp. 2d 909, 917 (D. Md. 2011).

The propriety of the CIA’s classification determinations is not for the defendant or the jury to decide. This is so because, even if information was mistakenly classified, that mistake has no bearing on whether the information was closely held which is the relevant inquiry for the jury. In other words, even if a particular document was labeled erroneously as “TOP SECRET,” so long as it was treated in accordance with the security measures required for material designated as such, it was still closely held for national security reasons and therefore could qualify as national defense information.

The Ninth Circuit addressed this distinction in *United States v. Lee*, 589 F.2d 980 (9th Cir. 1979), in the context of proposed testimony by a defense expert. In *Lee*, the defendant, charged with violating 18 U.S.C. §§ 793 and 794 (both of which have an NDI element), wanted to call an expert to “challenge the propriety of the classification” of certain documents marked “TOP SECRET.” *Id.* at 990. The Ninth Circuit found no error in the trial court’s exclusion of the expert’s

testimony finding “such an inquiry was totally irrelevant to the issues of th[e] case and of no help to the jury.” *Id.* The *Lee* Court noted that:

Under the espionage statutes charged in the indictment . . . , [the defendant] was found guilty of gathering and transmitting documents which relate to the “national defense.” There is no requirement in these statutes that the documents be properly marked “Top Secret” or for that matter that they be marked secret at all. It is enough that they related to the national defense and that they are transmitted with the intent to advantage a foreign nation or injure the United States.

Id. The same is true in this case.

Moreover, permitting inquiry and argument about whether the CIA’s classification decisions are correct would create tremendous risk that the jury would become confused or prejudiced because scrutinizing those classification decisions would necessarily require examining the underlying CIA intelligence-gathering activities that supported classification. As courts have found repeatedly, the details of the CIA’s intelligence-gathering activities are not proper subjects for the jury to consider and would only distract from the issues at trial. *See, e.g., United States v. Wilson*, 750 F.2d 7, 9 (2d Cir. 1984) (upholding trial court’s exclusion of defendant’s testimony about intelligence agency operations pursuant to Rule 403); *see also United States v. Anderson*, 872 F.2d 1508, 1519 (11th Cir. 1989) (“Whatever probative value that Carlisle’s participation in a prior covert operation had to this case, the admission of evidence regarding the details of those activities would only serve to impermissibly divert the jury’s attention away from the basic charges in this indictment.”). Thus, even if the defendant could point to some marginal probative value in the CIA’s alleged overclassification of any particular information, that probative value would be dwarfed by the risk of jury confusion or prejudice arising from a mini-trial related to the myriad of sensitive considerations that go into a particular classification determination.

Accordingly, the Government seeks an order from the Court precluding Schulte from eliciting testimony or arguing that the CIA improperly classified any specific piece of information. The Government does not object to Schulte seeking to introduce evidence that purportedly shows that the classified information that Schulte is charged with stealing was not in fact closely held, that it was not national defense information, or that Schulte did not intend or have reason to believe that the Classified Information would be used to the injury of the United States. But Schulte should not be permitted to elicit testimony from the Government's classification expert, Schulte's own classification expert, or any other witness about whether a particular document or piece of information is appropriately classified, and he should not be allowed to argue to the jury that the CIA misclassified any information.

The same goes for any argument that the CIA did not "under[take] . . . a legitimate classification review." (Sec. 6 Mot. at 44 n.21 (quoting Schulte's CIPA Sec. 5 Notice)). It is well-settled that the defendant "may not argue before the jury issues relating to the overall propriety of the Government investigation in this case [A]ny attempt by [the defendant] to dissect an individual law enforcement agent's state of mind during the course of the investigation, or to belabor the details of the investigation's chronological development, would be irrelevant to the central question of [the defendant's] guilt or innocence, and as such, is inadmissible." *United States v. Demosthene*, 334 F. Supp. 2d 378, 380 (S.D.N.Y. 2004) (citing *United States v. Regan*, 103 F. 3d 1072 (2d Cir. 1997); *United States v. Reyes*, 18 F.3d 65, 71 (2d Cir. 1994)). Similarly, the CIA's classification review nothing to do with the central question of the defendant's guilt.

VII. If Schulte's Expert Claims That the Government Withheld Information from Him, Then The Court Should Instruct the Jury That the Court Authorized the Government To Do So

In his expert notice, Schulte indicates that Steven Bellovin, his computer forensics expert, intends to testify to certain limitations on his ability to review evidence in this case, and to testify that he was not able to review all of the same material that was available to the FBI and the Government in the investigation of this case. While it is entirely proper for a defendant's expert to testify to the limitations of his review so that the jury can assess whether "the opinion of an expert was based on . . . sufficient data," Jury Charge, *United States v. Flores*, 15 Cr. 765 (PAC), the expert may not create the misleading impression that material was improperly withheld from the defendant or his expert. Indeed, the scope of the material to be produced to Schulte's expert has been the subject of extensive CIPA litigation, and the materials produced to the defendant, including the redactions to those materials, have been approved by the Court. Accordingly, should Schulte's expert testify that certain material was redacted or otherwise unavailable to him, the Government respectfully requests that the Court give the following limiting instruction at the conclusion of Bellovin's direct examination, derived from the text of CIPA:

You heard the witness testify that certain material was not available for him to review or that certain materials that he reviewed were redacted, meaning that parts of the materials were blacked out. You heard this testimony because it is up to you, as the jury, to determine whether an expert's opinions are based on sufficient data or expertise, and to determine what weight to give to the expert's opinions. You may not, however, consider why any material was not available to the witness to review. The reasons are not relevant to your determination of the facts of this case, and I instruct you that there was nothing improper about the fact that certain materials were not available to the defendant's expert. The Court has already determined that the materials provided to the defendant's expert, even if not exactly the same as the materials available to the Government, provide

the defendant with substantially the same ability to make his defense. You should not consider the fact that I have made that determination as an expression of my opinion regarding the facts of this case. It is your job and your job alone to decide the facts of this case. I remind you that the burden of proving the defendant's guilt beyond a reasonable doubt rests at all times with the Government.

VIII. The Government Provides Notice of Certain Areas of Cross-Examination and Extrinsic Evidence That May Be Implicated By Schulte's Testimony

Schulte's counsel has said on multiple occasions that Schulte intends to testify. The Government hereby provides notice that Schulte's testimony and/or arguments made by counsel will likely open the door to several areas of cross-examination and the introduction of certain extrinsic evidence of prior instances of Schulte's conduct.

A. Applicable Law

The Constitution guarantees a criminal defendant the right to choose whether or not to testify at trial. *See Harris v. New York*, 401 U.S. 222, 225 (1971). However, if a defendant testifies in his own defense, "his credibility may be impeached and his testimony assailed like that of any other witness, and the breadth of his waiver is determined by the scope of relevant cross-examination." *Brown v. United States*, 356 U.S. 148, 154-55 (1958). Indeed, "[i]t is essential . . . to the proper functioning of the adversary system that when a defendant takes the stand, the government be permitted proper and effective cross-examination in an attempt to elicit the truth," *United States v. Havens*, 446 U.S. 620, 626-27 (1980); *United States v. Spinelli*, 551 F.3d 159, 167 (2d Cir. 2008) ("By choosing to testify . . . the defendant gives up his right to refuse to answer questions that fall within the proper scope of cross-examination.").

As a result, "[w]hen a defendant offers an innocent explanation he 'opens the door' to questioning into the truth of his testimony, and the government is entitled to attack his credibility

on cross-examination.” *United States v. Payton*, 159 F.3d 49, 58 (2d Cir. 1998); *see also United States v. Desposito*, 704 F.3d 221, 234 (2d Cir. 2013) (“[w]hen a defendant offers an exculpatory explanation for the government’s evidence, he ‘opens the door’ to impeachment of his credibility, even by previously inadmissible evidence”); *United States v. Beverly*, 5 F.3d 633, 640 (2d Cir. 1993) (defendant’s testimony as to his unfamiliarity with guns opened the door to questioning about his prior possession and use of guns); *United States v. Garcia*, 936 F.2d 648, 654 (2d Cir. 1991) (“once [defendant] Dominguez testified that he had no idea that the white powder was cocaine, he opened the door for the Government to impeach his testimony by establishing on cross-examination that he was familiar with and indeed had used cocaine as recently as the day before his arrest”).

“A defendant has no right to avoid cross-examination into the truth of his direct examination, even as to matters not related to the merits of the charges against him.” *Payton*, 159 F.3d at 58. In *Garcia*, for example, the Second Circuit allowed cross-examination concerning the defendant’s marital history because of Garcia’s attempt on direct examination “to portray himself as a solid citizen with a stable family life.” *Id.* “The government need not offer extrinsic evidence to show that a defendant lied so long as it can point to a good-faith basis for its questions.” *Payton*, 159 F.3d at 59; *see also United States v. Katsougrakis*, 715 F.2d 769, 778-79 (2d Cir. 1983).

Like any other witness, the Court may also permit cross-examination of the defendant regarding “specific instances of conduct” concerning the defendant’s character for truthfulness. *See Fed. R. Evid. 608(b)* (but noting that “extrinsic evidence is not admissible to prove specific instances of a witness’s conduct in order to attack or support the witness’s character for truthfulness”). Importantly, however, the admission of extrinsic evidence to impeach a

defendant's testimony is not subject to analysis under Rules 608(b) or 404(b). Under the doctrine of "impeachment by contradiction," when "a witness puts certain facts at issue in his testimony, the government may seek to rebut those facts, including by resorting to extrinsic evidence if necessary." *United States v. Ramirez*, 609 F.3d 495, 499 (2d Cir. 2010); *see also* Fed. R. Evid. 608, advisory committee notes to 2003 amendments ("[T]he amendment leaves the admissibility of extrinsic evidence offered for other grounds of impeachment (such as contradiction, prior inconsistent statement, bias and mental capacity) to Rules 402 and 403."). "Thus, where a defendant testifies on direct examination regarding a specific fact, the prosecution may prove on cross-examination 'that [the defendant] lied as to that fact.'" *United States v. Garcia*, 936 F.2d 648, 653 (2d Cir. 1991) (quoting *United States v. Garcia*, 900 F.2d 571, 575 (2d Cir. 1990)). "The same holds true for defendant's false statements on cross-examination." *United States v. Beverly*, 5 F.3d 633, 639-40 (2d Cir. 1993).¹⁵ In addition, "the government's opportunity to impeach the defendant's credibility once he has taken the stand includes the opportunity to use evidence that it was barred from using on its direct case." *Id.* at 640.

Precisely because a defendant who testifies may not "frustrate the truth-seeking function of a trial by presenting tailored defenses insulated from effective challenge," the Government is afforded "great leeway" in its cross-examination of a defendant. *United States v. Vega*, 589 F.2d 1147, 1151 n.3 (2d Cir. 1978). Moreover, trial courts are "accorded broad discretion in controlling

¹⁵ In *United States v. Ramirez*, the Second Circuit characterized as dicta *Beverly's* application of the doctrine of contradiction to false statements on cross-examination. 609 F.3d at 500 n.1.

the scope and extent of cross-examination.” *United States v. Wilkerson*, 361 F.3d 717, 734 (2d Cir. 2004).

B. Discussion

Schulte’s testimony or arguments made by his counsel may open the door to several lines of cross-examination and the introduction of extrinsic evidence including, but not limited to, the following:

Law-abiding. If Schulte testifies or defense counsel argues that Schulte was a law-abiding citizen, the Government intends to cross-examine the defendant concerning (i) his possession and sharing of thousands of copyrighted electronic media; (ii) his statements to others that he “personally dont [sic] give a damn what the law says. I do whatever I think will benefit myself”; (iii) his statements to others that “if you’re going to break they [sic] law might as well go all out and just trample all over it”; (iv) his statements to others that “[l]egality of shit has absolutely no affect [sic] on me”; and (v) his statements that he hacked into others’ computer accounts. *See, e.g., Beverly*, 5 F.3d at 640 (where a defendant “testified on direct in a manner calculated to portray himself as a law-abiding musical performer who had nothing to do with guns,” the district court acted within its discretion “in allowing the government to elicit evidence of the shootings in order to discredit” the defendant’s “self-depiction”); *Garcia*, 936 F.2d at 653-54 (affirming cross-examination of defendant on his familiarity with cocaine and his marital history after the defendant “opened the door” on his direct testimony and attempted to “portray himself as an unwitting bystander” and “portray himself as a solid citizen with a stable family life”); *Payton*, 159 F.3d at

58 (affirming cross-examination to impeach credibility of defendant who testified that he “had nothing to hide” at the time of a search).¹⁶

Patriotism. If Schulte testifies or defense counsel argues that Schulte is a patriot and/or would never harm the United States, the Government intends to cross-examine Schulte concerning (i) his writings in the Schulte Notebooks, including his belief that the FBI is a “terrorist organization”; (ii) his statements to others that “I hope I live to see the day that Americans take up arms against the government”; (iii) his statements to others that “[i]t’s people like me that the gov’t will fear most” because “I will not falter on my beliefs and ideals”; and (iv) his statements in *pro se* court filings that he believes that Attorney General, the Department of Justice, the U.S. Attorney’s Office, the FBI, and the U.S. Supreme Court are all “federal terrorists.” *See, e.g., Beverly*, 5 F.3d at 640; *Garcia*, 936 F.2d at 653-54; *Payton*, 159 F.3d at 58.¹⁷

Bias. If Schulte testifies or defense counsel argues that Employee-1 or other employees were biased toward Schulte for improper reasons, the Government intends to cross-examine Schulte concerning racist statements made by Schulte to Employee-1 and others including, among other things, Schulte (i) referring to individuals of non-white descent as “towel heads,” “nigger

¹⁶ The Government does not intend to cross-examine Schulte concerning his possession of thousands of images and videos of child pornography or his possession of sexually explicit photographs of his unconscious female roommate, unless Schulte explicitly opens the door to such cross-examination. The Government will notify the Court and defense counsel out of the presence of the jury before pursuing those lines of cross-examination.

¹⁷ Depending on Schulte’s arguments at trial, the Government may seek to introduce Schulte’s statements identified above in the “Law-abiding” and “Patriotism” sections in its case-in-chief as Rule 404(b) evidence of his motive and intent. Indeed, in light of some of the arguments made by defense counsel in pretrial proceedings—including that Schulte was not disgruntled at the CIA and is a patriot who would have never harmed his country—it appears that Schulte’s defense will inevitably open the door to this evidence prior to his cross-examination.

bitch,” “sand niggers,” or “spics”; (ii) describing Arabic as “terrorist writing”; and (iii) stating that “[g]enocide is necessary to cleanse the human race” in reference to Mexicans. *United States v. Abel*, 469 U.S. 45, 50-51 (1984) (“A successful showing of bias on the part of a witness would have a tendency to make the facts to which he testified less probable in the eyes of the jury than it would be without such testimony.”); *see also* Fed. R. Evid. 611(b) (“Cross-examination should not go beyond the subject matter of the direct examination and matters affecting the witness’s credibility.”).

Past Mishandling of Classified Information. If Schulte testifies or defense counsel argues that Schulte never brought home documents from DEVLAN, the Government intends to cross-examine Schulte concerning statements he made to others that he downloaded data from CIA computer systems onto a CD and loaded it onto one of his servers at home. *See* Fed. R. Evid. 613(b); *United States v. Devine*, 934 F.2d 1325, 1344 (5th Cir. 1991) (“It is well-settled that evidence of a prior inconsistent statement is admissible to impeach a witness.”).

CONCLUSION

For the foregoing reasons, the Government respectfully submits that the Court should grant the relief requested herein.

Dated: New York, New York
November 25, 2019

Respectfully Submitted,

GEOFFREY S. BERMAN
United States Attorney for the
Southern District of New York

By: /s/
David W. Denton, Jr.
Sidhardha Kamaraju
Matthew Laroche
Assistant United States Attorneys
212-637-2744/6523/2420

Cc: Defense Counsel
(Via ECF)

PROFFER AGREEMENT

With respect to the meeting of Joshua Schulte ("Client") and his attorney, Mark Baker, Esq., with Assistant United States Attorney Matthew Laroche to be held at the Office of the United States Attorney for the Southern District of New York on November 16, 2017 ("the meeting"), the following understandings exist:

(1) **THIS IS NOT A COOPERATION AGREEMENT.** The Client has agreed to provide the Government with information, and to respond to questions, so that the Government may evaluate Client's information and responses in making prosecutive decisions. By receiving Client's proffer, the Government does not agree to make a motion on the Client's behalf or to enter into a cooperation agreement, plea agreement, immunity or non-prosecution agreement. The Government makes no representation about the likelihood that any such agreement will be reached in connection with this proffer.

(2) In any prosecution brought against Client by this Office, except as provided below the Government will not offer in evidence on its case-in-chief, or in connection with any sentencing proceeding for the purpose of determining an appropriate sentence, any statements made by Client at the meeting, except (a) in a prosecution for false statements, obstruction of justice or perjury with respect to any acts committed or statements made during or after the meeting or testimony given after the meeting; or (b) if, at any time following the meeting, Client becomes a fugitive from justice.

(3) Notwithstanding item (2) above: (a) the Government may use information derived directly or indirectly from the meeting for the purpose of obtaining leads to other evidence, which evidence may be used in any prosecution of Client by the Government; (b) in any prosecution brought against Client, the Government may use statements made by Client at the meeting and all evidence obtained directly or indirectly therefrom for the purpose of cross-examination should Client testify; and (c) the Government may also use statements made by Client at the meeting to rebut any evidence or arguments offered by or on behalf of Client (including arguments made or issues raised sua sponte by the District Court) at any stage of the criminal prosecution (including bail, all phases of trial, and sentencing) in any prosecution brought against Client.

(4) The Client understands and agrees that in the event the Client seeks to qualify for a reduction in sentence under Title 18, United States Code, Section 3553(f) or United States Sentencing Guidelines, Sections 2D1.1(b)(16) or 5C1.2, the Office may offer in evidence, in connection with the sentencing, statements made by the Client at the meeting and all evidence obtained directly or indirectly therefrom.

(5) To the extent that the Government is entitled under this Agreement to offer in evidence any statements made by Client or leads obtained therefrom, Client shall assert no claim under the United States Constitution, any statute, Rule 410 of the Federal Rules of Evidence, or any other federal rule that such statements or any leads therefrom should be suppressed. It is the intent of this Agreement to waive all rights in the foregoing respects.


(6) If this Office receives a request from another prosecutor's office for access to information obtained pursuant to this Proffer Agreement, this Office may furnish such information but will do so only on the condition that the requesting office honor the provisions of this Agreement.


(7) It is further understood that this Agreement is limited to the statements made by Client at the meeting and does not apply to any oral, written or recorded statements made by Client at any other time. No understandings, promises, agreements and/or conditions have been entered into with respect to the meeting other than those set forth in this Agreement and none will be entered into unless in writing and signed by all parties.

(8) The understandings set forth in paragraphs 1 through 7 above extend to the continuation of this meeting on the dates that appear below.

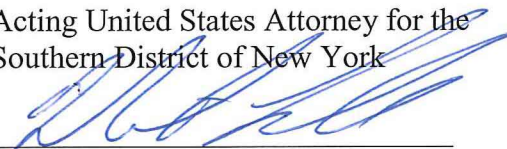
(9) Client and Attorney acknowledge that they have fully discussed and understand every paragraph and clause in this Agreement and the consequences thereof.


Dated: New York, New York



Client


Attorney for Client

JOON H. KIM
Acting United States Attorney for the
Southern District of New York
by: 

Assistant United States Attorney


Witness

Dates of Continuation

Initials of counsel, Client, AUSA, witness

